



GBBC

Global Blockchain
Business Council

BLOCKCHAIN FOR GOOD

Real-world use cases supporting the
UN Sustainable Development Goals (SDGs)

*81st Session of the United Nations
General Assembly*

2026 Edition



TABLE OF CONTENTS

Food for Crisis	2
Digital Certificate of Entitlement	10
Decentralized Trusted Lists for Digital-ID Interoperability in Latin America	18
The Biocultural Jaguar Credit	26
Occidental (Oxy) Open Sourcing the Verra CCS+ Master Extension Set	32
Configurable Infrastructure for Onchain Lending	41
GBBC's 101 Real-World Blockchain Use Cases Handbook	50

SECTION I

FOOD FOR CRISIS

WITH GBBC GIVING & WORLD FOOD
PROGRAMME INNOVATION ACCELERATOR



FOOD FOR CRISIS OVERVIEW

Food for Crisis was a collaborative initiative developed between 2023 and 2025 by the **World Food Programme (WFP) Innovation Accelerator** and **GBBC Giving**, a nonprofit organization under the aegis of **Global Blockchain Business Council**. The initiative explored how **blockchain** and **Web3** approaches could strengthen transparency and accountability in humanitarian financing, particularly by improving traceability of funds from donor to end beneficiary.

The initiative was designed in response to rising and increasingly complex food insecurity needs. The UN's flagship **State of Food Security and Nutrition in the World 2025 (SOFI 2025)** estimates that **around 673 million people experienced hunger in 2024**, equivalent to **about 8.2 percent** of the global population (with progress uneven across regions, including continued deterioration in parts of Africa and Western Asia). In parallel, WFP's operational environment continues to be shaped by conflict, climate shocks, and economic instability, with acute food insecurity affecting hundreds of millions of people.

Food for Crisis examined how emerging digital technologies could improve end-to-end traceability of humanitarian transactions and reporting, with the aim of reducing inefficiencies, strengthening donor confidence and enabling clearer visibility across the delivery chain. Conceptually, it proposed a **blockchain agnostic** approach capable of tracing both **fiat and digital asset** flows in near real time, with a longer-term vision of an **open-source dashboard** integrating multiple payment rails and platforms.

FOOD FOR CRISIS PROOF-OF-CONCEPT IN PERU

Starting in November of 2024, Food for Crisis implemented a Proof-of-Concept (PoC) at the WFP Country Office in Peru, with WFP staff in collaboration with the Swiss-based technology company AIDONIC. The pilot tested an NFT-based traceability solution designed to record and verify humanitarian fund flows from donor to recipient. The solution combined decentralized storage, tokenized data integrity and privacy-preserving, end-to-end transparency to demonstrate how emerging technologies can strengthen trust, improve accountability and enhance efficiency in aid delivery.

The PoC used Filecoin's decentralized storage network and blockchain to mint NFTs that immutably recorded donation and distribution data. The process represented fiat donations as digital twins on the blockchain, enabling tracking without using on-chain financial transfers.



AIDONIC workshop participants (Photo: WFP/Peru)

NFT Traceability Solution

AIDONIC's ImpactNFT system created an end-to-end traceable chain of accountability by connecting the *First Mile* (donation management) with the *Last Mile* (aid distribution). The solution includes:

Two Types of NFTs

These NFTs allow both donors and aid organizations to maintain transparent, verifiable, and tamper-proof records of aid activities.

1) Donor NFT - Serves as an immutable record of a donor's contribution.

- Contains metadata about the donation, images or project visuals, and a summary of the donation's impact
- Includes a QR code linking to the donation receipt and related updates

2) Distribution NFT - Owned by the aid organization, representing the verified distribution of aid.

- Includes metadata and blockchain verification details
- Contains a QR code linking to a detailed distribution report saved on decentralized storage that records each recipient transaction and other details of the distribution, keeping the necessary level of individual privacy

Verification and Data Integrity

The Last-Mile platform ensures the accuracy and authenticity of distribution data through:

- Automated capture of time, date, and GPS location data during distributions
- Possibility of integration with financial partners for digital cash transfers
- Optional facial recognition for recipient verification
- Real-time synchronization with blockchain technology
- Decentralized, tamper-proof storage using Filecoin

Privacy and Security

While transparency is central, the system maintains strict data privacy through the following:

- Personally identifiable information (PII) is kept off-chain and separate from public records
- Transactions use unique identifiers to protect recipient identity
- Visibility settings can be customized for different stakeholders

RESULTS AND LEARNINGS

The PoC in Peru demonstrated the technical feasibility of using NFTs for humanitarian aid traceability. The pilot validated that blockchain technology can create verifiable, tamper-proof records of humanitarian assistance while protecting recipient dignity and privacy. Key takeaways show that the project confirmed the potential of blockchain and decentralized storage to strengthen humanitarian aid systems in the following ways:

End-to-End Transparency

The NFT-based system successfully linked donation and distribution records through blockchain and decentralized storage, providing a clear, auditable chain of transactions.

Enhanced Donor Engagement

Donors could track the impact of their contributions in real time, fostering trust and ongoing participation, building trust and encouraging continued support.

Data Protection

Privacy-preserving architecture met the dual objectives of accountability and beneficiary security, ensuring sensitive information remained protected.

Potential for Operational Integration

The system showed flexibility to connect with traditional financial rails (e.g., mobile money, bank transfers), demonstrating readiness for future scale-up and integration into existing workflows.

FUTURE OPPORTUNITIES

Following the success of the PoC in Peru, there are promising opportunities to use blockchain and decentralized storage technology for humanitarian aid, especially in the following ways:

- Integration across blockchain networks and stablecoin systems for broader traceability coverage
- Development of an open-source, blockchain-agnostic dashboard capable of aggregating data from multiple platforms
- Expansion of pilots across different regions and types of humanitarian aid
- Potential applications beyond food aid — including economic development, financial inclusion, and remittance tracking

In the long-term, a global traceability framework could ensure every donation, whether in fiat or crypto, is transparently tracked, while keeping a privacy-first mindset. This would require continued testing, deployments, and collaboration across major stakeholders.



AIDONIC workshop participants (Photo: WFP/Peru)

CONCLUSION

Under the Food for Crisis initiative, the AIDONIC NFT Proof-of-Concept in Peru demonstrated the real potential of traceability based on blockchain and decentralized storage technology to improve the efficiency and integrity of humanitarian aid. By combining transparent, tamper-proof records with strong safeguards for recipient privacy, the model offers a scalable pathway towards a higher standard of global aid accountability. The initiative highlights how public-private collaboration and Web3 innovation can generate measurable impact in tackling food insecurity and supporting economic development, while contributing directly to the achievement of UN Sustainable Development Goal 2: Zero Hunger.



AIDONIC workshop participants (Photo: WFP/Peru)

SECTION II

DIGITAL CERTIFICATE OF ENTITLEMENT

*A blockchain-based digital identity solution for
global proof-of-life verification*

WITH UNITED NATIONS JOINT STAFF PENSION
FUND (UNJSPF), DEVELOPED WITH THE
UNITED NATIONS INTERNATIONAL
COMPUTING CENTRE (UNICC)



PROBLEM BEING ADDRESSED

For more than 70 years, the United Nations Joint Staff Pension Fund (UNJSPF) relied on a paper-based Certificate of Entitlement to confirm annually that retirees and beneficiaries remained eligible for pension payments. The Fund serves more than 80,000 retirees and beneficiaries dispersed across over 190 countries and jurisdictions. Each individual had to receive, sign and return a physical proof-of-life form, often through postal systems that varied greatly in speed and reliability.

The limitations were material. Postal delays, lost documents, manual signature checks and archiving requirements created administrative bottlenecks and uncertainty for beneficiaries. The risks were most acute for people living in remote locations, conflict-affected areas or countries with limited postal and digital infrastructure. The COVID-19 disruption further demonstrated the fragility of a process dependent on international mail. An undelivered certificate could contribute to benefit suspension and a lengthy reinstatement process.

The Fund also needed stronger identity assurance. A handwritten signature offered limited protection against impersonation, document manipulation or identity fraud. In addition, the Fund must sometimes validate residence information in administering the two-track pension adjustment system. The challenge was therefore broader than digitizing a form. UNJSPF needed a globally scalable, privacy-preserving and auditable trust system capable of establishing four proofs: identity, life, transaction and, where required, location.

HOW THE SOLUTION WORKS

80K

retirees &
beneficiaries

190+

countries &
jurisdictions

43K

active digital
users

99.96%

user
retention

UNJSPF and UNICC developed the Digital Certificate of Entitlement (DCE) as an optional digital alternative to the paper process. The mobile solution combines decentralized identity, blockchain, artificial intelligence, facial biometrics, active liveness detection and geolocation. Beneficiaries can use a smartphone or tablet to establish a digital identity and complete the annual proof-of-life exercise without mailing a paper form.

The DCE is built on Hyperledger Indy and Aries. A permissioned distributed ledger provides the trust layer for decentralized identifiers and cryptographic verification. The ledger does not store raw facial images, biometric templates or other personally identifiable information. Instead, it records decentralized identifiers and cryptographic proof metadata, creating a tamper-evident and auditable record without turning the blockchain into a repository of sensitive personal data.

Identity and biometric processing are designed around data minimization. Facial matching, liveness checks and presentation-attack controls are executed at the edge, on the beneficiary's device, with biometric information protected in the device's secure environment. The blockchain anchors proof of transaction and supports verification of credentials, while geolocation can support proof of location when Fund rules require residence validation. Together, the technologies address the four pillars of pension entitlement verification.

The Four Verification Pillars

1. Proof of Identity

Confirms that the claimant matches the registered beneficiary.

2. Proof of Life

Uses active liveness and presentation-attack mitigation to confirm physical presence.

3. Proof of Transaction

Creates immutable, tamper-evident cryptographic validation without exposing personal data.

4. Proof of Location

Supports residence validation as required for two-track pension calculations.

The architecture also addresses the gap between deterministic ledgers and probabilistic AI. A blockchain can preserve a verification result immutably, but biometric AI produces confidence-based outputs that can drift or be attacked. The DCE therefore combines active liveness at the edge, independent verification controls and human review. Low-confidence cases are routed to caseworkers rather than automatically rejected, helping prevent an automated mismatch from causing an inappropriate pension suspension.

Accessibility remains central. The digital channel is voluntary and the paper process remains available. For beneficiaries without a suitable smartphone or reliable connectivity, UN field-office kiosks extend access to the DCE. This multichannel model recognizes that digital transformation must reduce exclusion rather than create a new barrier.

RESULTS AND LEARNINGS

The DCE moved from a 2020 pilot involving 351 participants in 43 countries to production rollout in 2021. By 2025/2026, more than 43,000 beneficiaries were active digital users, representing over 60 percent adoption. User retention reached 99.96 percent, with only 15 users returning to the paper process. Paper-based processing declined by 40 percent, archiving costs fell by more than 95 percent, and annual peak overtime expenses decreased by 76.5 percent.



The operational results demonstrate that blockchain can create value without a token, cryptocurrency or public mining model. In this use case, distributed ledger technology provides a controlled, auditable and tamper-evident trust layer for identity transactions. The larger benefits arise from the complete service design: privacy-preserving identity, edge biometrics, automated workflows, human oversight and inclusive access channels. A central lesson is that trust must be engineered, not assumed.

UNJSPF has aligned the solution with GBBC's Capital Markets Risk Mitigation Framework and a multi-standard assurance approach spanning ISO/IEC 27001 for information security, ISO/IEC 27701 for privacy information management, ISO/IEC 42001 for AI management, and ISO/IEC 30107-3 for biometric presentation attack detection. The assurance model addresses risks including deepfake injection, key or device loss, immutable exposure of personal data, cloud outages and audit reconciliation.



DCE for beneficiaries (Photo: UNJSPF)

A second lesson is that privacy and security can reinforce each other. Strong identity assurance does not require centrally warehousing biometric data or placing personal information on an immutable ledger. A third lesson is that AI governance is part of identity governance. Model performance, bias mitigation, confidence thresholds, drift monitoring and escalation to human decision-makers must be managed throughout the system lifecycle. Finally, collaborative governance is essential for scale: shared standards, common controls and reusable infrastructure can reduce duplication across institutions.

FUTURE OPPORTUNITIES

The DCE has become a practical blueprint for a broader UN digital identity ecosystem. The platform's decentralized identity and wallet concepts can support portable, verifiable credentials across an individual's relationship with the UN system, from organizational processes through retirement. A multi-agency shared-service model could allow participating organizations to use a pre-assured platform, share costs and jointly shape the product roadmap.

The technical roadmap also addresses emerging risks. UNJSPF is exploring migration of cryptographic foundations toward NIST-standardized post-quantum algorithms to reduce long-term exposure to 'harvest now, decrypt later' threats. Another opportunity is periodic public anchoring, in which a Merkle root representing the state of the permissioned ledger could be recorded on a public blockchain. Such anchoring could provide externally verifiable tamper evidence without disclosing private transactions or personal data.

The identity wallet could also evolve into a fuller pension application supporting secure document submission and, subject to appropriate governance and controls, potential digital payment services. Beyond pensions, the DCE model is relevant to social protection, humanitarian assistance and other public services that require reliable proof of identity, presence and entitlement across borders.

The DCE ultimately demonstrates a pragmatic role for blockchain as digital public infrastructure. Its value lies not in replacing institutional responsibility, but in strengthening it through verifiable records, privacy-preserving architecture, rigorous assurance and collaborative governance. The experience can be summarized in three principles: trust is engineered, privacy and security must coexist, and shared governance unlocks scale.

SECTION III

DECENTRALIZED TRUSTED LISTS FOR DIGITAL-ID INTEROPERABILITY IN LATIN AMERICA

WITH AVA LABS



PROBLEM BEING ADDRESSED

One of the main factors limiting the interoperability of trust services in Latin America and the Caribbean (LAC), such as the verification of digital credentials, is the absence of a regional trust registry that makes it possible to validate, across borders, each country's trusted issuers, and to manage the revocation and suspension states of digital credentials. This same problem has limited the interoperability of electronic signatures between countries in the region for more than a decade, and it takes on significantly greater relevance in scenarios of cross-border verifiability of digital identity documents.

A digital ID issued in one country works well domestically, but the moment a bank, government agency, or verifier in another country encounters it, there is no trust registry against which to confirm who issued it or whether it is still valid. Cross-border trust requires answering two questions at the moment of verification: who issued this identity, and is it still valid right now. The European Union addressed this through eIDAS2 trust lists; the United States has no binding regional framework; and LAC has neither a shared registry nor a neutral regional operator with a mandate to run one.

OVERVIEW OF HOW THE SOLUTION WORKS

AGESIC, Uruguay's e-government agency, and Blerify designed and implemented a pilot in Uruguay that integrates all the key components for issuing and verifying digital government documents as verifiable credentials in an identity wallet, following the ISO/IEC 18013-5 and OpenID4VP standards. In a pioneering move for the region, the pilot used a trust list deployed on smart contracts on the Avalanche and LNet blockchain networks, evaluated as a scalable alternative to the infrastructure, governance, and sovereignty challenges required to enable regional interoperability of digital identity in LAC.

The end-to-end pilot

The project ran across five phases: defining and configuring AGESIC and trusted issuer UrulD; generating Uruguay's trusted list on-chain; configuring and issuing the digital ID credential to pilot participants by email; authenticating with the digital ID against a demo of the Uruguay ID Broker via OpenID4VP, using a QR code scan approved on the participant's phone; and, finally, testing real-time updates, key rotation, and revocation, confirming that credential and issuer status changes propagated live to any entity subscribed to the smart contract's events, in Uruguay and abroad.

A decentralized list of lists

The smart-contract layer enables a highly useful element for international interoperability: each country can operate its own smart contract on a server (node) that stays in sync with those of other countries. The pilot used two sets of smart contracts, one for the issuer trusted list and one for credential status, deployed across Avalanche and LNet, a Latin American and Caribbean enterprise blockchain network.

AGESIC created and managed the trust-list and revocation-list smart contracts and approved trusted issuers including UrulD, a test issuer that issued and revoked identity credentials as mDocs under ISO/IEC 18013-5. Blerify operated the identity-as-a-service infrastructure, the Blerify ID Wallet (iOS and Android), and the Blerify Credential Management Platform used to configure service accounts, define credential look and feel, and manage trusted lists via web interface or API.



The AGESIC and Blerify teams (Photo: Blerify)

Why blockchain, specifically

Blockchain provides the one capability none of the alternatives could match: a tamper-proof, continuously synchronized record that no single operator controls. Each country runs its own node, hosted on national cloud, government infrastructure, or on-premise, and only that country can edit its own list, authenticated through its own DID, X.509 certificate, and keys. Every node holds a synchronized copy of the full regional list, with changes propagating automatically in roughly two seconds through event subscriptions, preventing a single point of failure, a single point of capture, and any one party holding a central switch. The blockchain itself never stores credentials, identity attributes, biometrics, or other personal data; it stores only trust metadata, issuer identifiers, public keys, and cryptographic credential-status entries.

RESULTS AND LEARNINGS

The pilot validated, end to end, that a government-issued digital identity can be issued, verified, rotated, and revoked across a decentralized regional trust registry, with no personal data ever touching the chain.

Real-Time Regional Propagation

Credential and issuer status changes, including key rotations and revocations, propagated automatically in about 2 seconds to any entity subscribed to the smart contract's events, in Uruguay and abroad.

Zero Personal Data On-Chain

The blockchain carried only issuer metadata and cryptographic credential-status entries, never biometric data, identity attributes, or credentials themselves, keeping the chain privacy-safe by design.

Sovereignty Without a Central Operator

AGESIC and UrulD each registered their own DID, X.509, and public key directly in a smart contract within a synchronized network, proving cross-border trust does not require ceding control to a central operator.

Recognized Globally

The project won the Digital Public Infrastructure (DPI) Government Hackathon organized by CDPI and was awarded in South Africa in November 2025 during the Global DPI Summit 2025.

A structured comparison of bilateral, centralized, and decentralized trust-list models, developed as part of the case study, found the decentralized approach scores highest on sovereignty, resilience to failure or capture, audit and traceability, and scalability to the private sector, while trailing centralized models only on current regulatory acceptance and standardization maturity, since a decentralized

regional registry is still an emerging model with few precedents in LAC.

**Blerify Co-Founder & COO
Andrew Piscione with the LAC
DPI Community at 2025 DPI
Summit, South Africa**
(Photo: Blerify)



It is worth pointing out that hardest part of the interoperability problem is not technical, but a governance problem. A single central registry is politically unworkable in the region because it would require every country to cede control of its trust infrastructure to one operator, and LAC currently has no neutral regional body with a mandate to run one. The decentralized, node-per-country model exists specifically to solve that. Any government or partner considering a similar path should define upfront who can deploy a node, what technical and security requirements a node must meet, and what regulatory decree will recognize the trusted list as a valid information registry, since rules agreed once can be encoded directly into the permissioning logic of the network itself.

Comparing Trust-List Models for Cross-Border Digital Identity

Bilateral vs. centralized vs. decentralized — from the AGESIC-Blerify pilot case study

Criterion	Bilateral (no regional list)	Centralized	Decentralized (piloted)
Regional interoperability	Low peer-to-peer	High common registry	High no central operator
Sovereignty & national control	High but isolated	Low ceded to operator	High own node & list
Maturity & standardization	—	High proven (EU/ETSI)	Emerging few precedents
Regulatory acceptance today	Case by case	High fits PKI frameworks	To be built requires decrees
Resilience to failure/capture	Low single point of failure	Medium single point of failure	High no single point
Operator dependency	None	High neutral operator absent	None avoids lock-in
Audit & traceability	Low depends on setup	Medium depends on operator	High immutable history
Change propagation	Manual and slow	Medium depends on operator	Automatic ~2s, event-based
Scalability to private sector	Low hard to expose registry	Low hard to expose registry	High public registry by nature
Governance	Bilateral scales one-to-one	Centralized mandated body	Distributed rules coded in

● Advantage ● Intermediate / conditioned ● Limitation ● Not applicable

Comparison of trust-list models across ten criteria (Photo: Blerify)

FUTURE OPPORTUNITIES

AGESIC has presented this pilot as an open contribution rather than a finished product, and is seeking funding to develop the smart-contract infrastructure into an open-source Digital Public Good, with documentation and deployment scripts so any LAC country can stand up its own node. Promising next steps include:

- Formalizing governance through a neutral regional body to coordinate which countries and entities can connect to the network and to run incident-management protocols.
- Defining the regulatory decrees each participating country needs to recognize the decentralized trusted list as a valid information registry for digital credentials and other trust services such as electronic signatures.
- Integrating the model with the Ciudadano Digital LAC (IdLAC) initiative and enabling OpenID4VP in a model broker, so verifiable credentials can automatically authenticate across the region, including cross-border use.
- Extending the same architecture beyond national ID to birth certificates, health records, academic diplomas, and other credential types, each with country-specific validation rules.
- Growing the network issuer by issuer and country by country, positioning Latin America and the Caribbean as an interoperable bloc as the EU, US, Canada, Australia, and India converge on digital identity standards.

SECTION IV

THE BIOCULTURAL JAGUAR CREDIT

WITH FUNDACIÓN PACHAMAMA &
REGEN NETWORK



PROBLEM BEING ADDRESSED

The Amazon rainforest is one of Earth's most vital ecosystems, playing a critical role in maintaining global biodiversity and regulating the planet's climate. However, this irreplaceable resource faces escalating threats from deforestation, habitat destruction, and climate change. Regen Network, in partnership with Indigenous communities and allies including Fundación Pachamama, is leveraging cutting-edge blockchain technology to address these challenges through innovative and regenerative solutions.

OVERVIEW OF HOW THE SOLUTION WORKS

A cornerstone of our work in the Amazon is our collaboration with the Sharamentsa and the broader Achuar Nation. This partnership places Indigenous wisdom and ancestral land stewardship at the heart of ecological preservation. The Sharamentsa community has long protected their biodiverse territories, including jaguar habitats and pristine rainforests, ensuring the vitality of these ecosystems for generations.

Regen Network amplifies their efforts by providing the tools and infrastructure to tokenize ecological assets while respecting their sovereignty over the design, deployment, and management of these assets. Regen, Sharamentsa, and allies worked together to develop the Biocultural Unit Paradigm.

As Regen Network Development CEO Gregory Landua explained, *"...Biocultural Units are a profound theory of reweaving relational value, symbolizing a harmonious balance between human activities and the Earth's ecosystems. This initiative heralds a shift towards more equitable, transparent, and effective mechanisms for environmental stewardship, grounded in the principles of ancestral wisdom and collaborative partnership."*

The Biocultural Jaguar Credit system exemplifies this integrated approach, linking cultural and ecological conservation by safeguarding approximately 10,000 hectares of jaguar habitat. Each credit represents a measurable commitment to preserving biodiversity while aligning with the values and traditions of the Achuar Nation.



Members of the Sharamentsa and Achuar Nation (Photo: Fundación Pachamama)

By facilitating transparent and equitable relationships between Indigenous communities, buyers, scientists, conservation organizations, and institutions, the project resolves longstanding challenges that have historically plagued interactions between Indigenous stewards and global organizations. The credit design ensures that the value generated directly benefits these communities, empowering them as equal partners in global ecological markets.

This initiative with Fundación Pachamama is strengthened through deep partnerships with organizations such as Stoknes Futures and the Amazon Sacred Headwaters Alliance. After a successful launch of the pilot, IDB Lab and NaturaTech LAC have joined our coalition to support program expansion to neighboring communities, in an effort to hold the line against road encroachment into Indigenous territories. These allies work in concert to support the Sharamentsa and Achuar Nation, combining technical expertise, cultural advocacy, and ecological strategies to ensure the success and scalability of the project. Together, these collaborations create a robust network that integrates Indigenous leadership, conservation science, and technological innovation.



Members of the Sharamentsa and Achuar Nation (Photo: Fundación Pachamama)



Members of the Sharamentsa and Achuar Nation *(Photo: Fundación Pachamama)*

HOW IT LEVERAGES BLOCKCHAIN

At the heart of Regen Network's efforts is its powerful Regen Ledger, an open-source, decentralized blockchain purpose-built for ecological markets. Regen Ledger provides the infrastructure needed to securely store, verify, and exchange ecological data, ensuring transparency, accountability, and trust among all stakeholders. It serves as the foundational platform for tools such as the Ecocredit Module, which facilitates the creation, verification, and trading of ecological credits; and the Regen Data Stream, a robust data pipeline that integrates satellite imagery, ground-truth observations, and scientific inputs to verify ecological outcomes in real time.

Together, these technologies create an ecosystem of trust and scalability that empowers communities, organizations, and investors to collaborate effectively in the preservation and regeneration of ecosystems.

FUTURE OPPORTUNITIES

This approach addresses more than ecological concerns; it also creates sustainable economic opportunities for the Sharamentsa and other Indigenous communities. By funding their unparalleled stewardship of the land, these communities secure a sustainable income stream that reinforces their role as guardians of the Amazon.

The model ensures a balance between local economic development and environmental regeneration, creating a template for equitable, long-term sustainability. To date, the Biocultural Strategy group has facilitated the sale of approximately \$132,000 worth of Biocultural Jaguar Credits, further validating the model's ability to connect Indigenous stewardship with real-world ecological markets.

Looking forward, Regen Network, Fundación Pachamama, and the Biocultural Jaguar Strategy group remain committed to scaling these efforts, deepening partnerships, and exploring new applications of blockchain to amplify Indigenous-led stewardship and planetary regeneration. Together, we can ensure the Amazon thrives and continues to provide the rest of society with clean air, water, and the depth of biological and cultural diversity Earth needs for a resilient future.

SECTION V

OCCIDENTAL (OXY) OPEN SOURCING THE VERRA CCS+ MASTER EXTENSION SET

WITH OXY





What a reusable digital methodology template based on GBBC initiative InterWork Alliance (IWA)'s digital Measurement Reporting and Verification (dMRV) Framework can do to accelerate trusted carbon markets, reduce implementation cost, and improve the integrity of carbon capture and storage credits.

PROBLEM BEING ADDRESSED

Carbon markets depend on trust: buyers need confidence that each credit represents a real, measurable, independently verified climate impact, while project developers need an efficient path to convert project activity into financeable environmental assets. For carbon capture and storage projects, that challenge is amplified by technical complexity.

The Verra VM0049 Carbon Capture and Storage methodology and its digital counterpart available on the Verra Project Hub, applies globally to CCS activities and relies on multiple modules and tools covering capture, transport, storage, electricity emissions, non-VCS CO₂ accounting, and differentiation between reductions and removals. That modular structure is valuable because it can support different project designs, but it also creates a high burden for data consistency and verification.

Historically, much of the measurement, reporting, and verification process has been document centric. Methodologies are expressed in PDFs, calculations are interpreted by implementation teams, and each project may recreate similar data structures, workflows, and evidence packages. This can slow project onboarding, introduce avoidable interpretation differences, increase verification effort, and limit interoperability between registries, verification bodies, suppliers, marketplaces, and digital platforms. Though much of these issues are addressed by the digital methodology on the Verra ProjectHhub, the business problem still exists on how to make that digitization, auditable by multiple project entities such as project proponents, VVBs, registries without rebuilding the same foundation each time.

OVERVIEW OF HOW THE SOLUTION WORKS

The Verra CCS+ Master Extension Set addresses this gap by translating methodology-specific requirements into reusable, machine-readable templates aligned with IWA's digital Measurement, Reporting, and Verification (dMRV) Framework. In the dMRV Framework, Extension Sets are groupings of templates that encompass entities, messages, formulae, and variables specific to the quality standard or methodology that a project is using. They can be organized into modules that act as shared libraries, allowing participants to use consistent digital representations of methodology requirements while still configuring them for the needs of a specific project.

A Master Extension Set functions like a common business language for the supplier, validation and verification body, and issuing registry. The open specification defines templates for equations (formulas), parameters (variables), entity extensions, and request/response message pairs. In the original methodology documentation, equations and parameters describe how project emissions and removals are calculated. In the digital implementation, those become Formula Templates and Variable Templates with fixed identifiers, descriptions, versions, units of measure, data schemas, and data examples. This means that when a supplier reports a value such as a mass flow measurement, the verifier and registry can process the same data element with a shared understanding of what it means, where it belongs, and how it contributes to a calculation.

Master Extension Set

Identity

ID

Name

Version

Description

Documentation

8cc9aed1-5f8e-41d8-9f18-353a12e18394

Verra's VM0049 CCS+ Master Extension Set Template

1.0

Extension set for carbon capture and storage (CCS) projects

<https://verra.org/methodologies/vm0049-carbon-capture-and-storage/>

Edit

Create Extension Set from this Master

Create Extension Set

Master Extension Set Modules (8)

Name	Version	Description	ID	
VMD0059	1.0	VMD0059 CO2 Capture FROM Bioenergy (BECCS)	1ef1d556-5bea-42ae-826a-01c236a8f3cc	View / Edit
VMD0062	1.0	VMD0062 CO2 Capture FROM Natural Gas Processing	c928df96-6dd3-4cad-babd-1433382b0642	View / Edit
VT0012	1.0	VT0012 Accounting Non-VCS CO2 in CCS Projects	4e1ce423-c1a4-43c3-a288-38d3a73e779a	View / Edit
VT0013	1.0	VT0013 Differentiating Reductions and Removals in CCS Projects, v1.0	0b1bc4f4-ceed-4431-8e89-4ea86aaf59c	View / Edit
VM0049	1.0	Carbon Capture and Storage (CCS) module	b4e1f1a9-1fd9-4fac-a538-6e25051a419b	View / Edit
VMD0056	1.0	Direct Air Capture (DAC) module	76122f3d-ac2e-429e-af3d-7e248f072eef	View / Edit
VMD0057	1.0	CO2 Transport for CCS Projects module	b37b6e9c-e959-4fa2-9bb8-c89ae0d489dd	View / Edit
VMD0058	1.0	VMD0058 CO2 Storage in Saline Aquifers and Depleted Hydrocarbon Reservoirs	991cfac7-babe-4667-a7a9-da28e7f083ee	View / Edit

The release to open source is the key business accelerator. Rather than each CCS project or platform independently interpreting the same methodology and rebuilding data contracts, the open Master Extension Set provides a reusable starting point. It can be installed into an implementation such as the Environmental Credit Service or adapted by other dMRV-aligned platforms. A project then creates its own project-specific Extension Set instance from the master templates, selects the modules it needs, and configures defaults such as units of measure, environmental variables, and project-specific reporting requirements.

The current Extension Set is integrated with the digital methodology on the Verra Project Hub via Rest APIs and creates set of documents such as Project Description, Monitoring Report, Validation Report and Verification Report as required by the VCS Standard. Once the data is received via the master Extension Set, the Verra Project Hub also runs its own calculation to ensure that the ERR values match. Multiple rounds of integration and accuracy testing have been conducted using a simulated yet complete data to ensure the robustness of the entire system.

HOW IT LEVERAGES BLOCKCHAIN

Blockchain and ledger platforms are used as the trust and coordination layer for the digital MRV process. As evidence is collected, submitted, reviewed, and verified, important events and attestations can be cryptographically linked to create a transparent chain of custody. The goal is not to put every operational data point on chain, but to establish provenance, integrity, and accountability across the lifecycle of the claim. Evidence can be secured so that its authenticity is verifiable, checkpoints can be recorded as part of a shared workflow, and verified claims can be traced through issuance, retirement of underlying claims, and distribution of the resulting environmental credit.

For business stakeholders, this improves market confidence in three ways. First, it makes the lineage of a credit easier to inspect because the origination process is digitally traceable. Second, it reduces ambiguity by anchoring the project's data to agreed templates and shared identifiers. Third, it supports automation because suppliers, verifiers, and registries can exchange structured messages and independently process the same formula and variable definitions. The result is a more scalable pathway for generating high-quality digital environmental assets while preserving the oversight roles that buyers and regulators expect.

RESULTS AND LEARNINGS

The Verra CCS+ Master Extension Set demonstrates that a complex CCS methodology can be converted into reusable digital infrastructure. The implementation described in the source material includes 105 Master Formula templates and 336 Master Variable templates across five modules and two toolsets, created through a real-world supply chain supporting carbon dioxide removal credit origination for a large direct air capture facility. **That scale matters: it shows that the approach can handle the depth of methodology content needed for a production-grade use case rather than a narrow proof of concept.**

The biggest learning is that standardization and flexibility must be designed together. A master set creates consistency, but projects still need to select modules, configure assumptions, and capture project-specific evidence. The Master Extension Set approach supports both requirements: it preserves consistent identifiers, schemas, and calculation templates while allowing each project to instantiate and configure the pieces it needs.

A second learning is that collaboration across the supplier, verifier, and registry is essential. The Extension Set is most valuable when it reflects the common operating model of the full supply chain, not just the interpretation of one participant.

A third learning is that open-source release can turn implementation work into market infrastructure. The effort invested in digitizing formulas, variables, workflows, and entity extensions becomes reusable by other CCS projects using the same methodology and can serve as a reference pattern for other methodologies. This creates a compounding benefit: every new implementation can start closer to production readiness, while feedback from additional projects can improve the shared resource over time.

FUTURE OPPORTUNITIES

The open-source Verra CCS+ Master Extension Set creates several near-term business opportunities. First, it can reduce onboarding time and implementation cost for CCS projects by giving teams a tested library of digital templates. Second, it can improve the quality and consistency of verification by giving VVBs structured evidence, repeatable calculations, and clear data contracts. Third, it can support interoperability between digital MRV platforms, the Verra Project Hub, registries, and exchanges by establishing common representations for methodology requirements.

Longer term, the same pattern can be extended beyond CCS. Other quality standards and methodologies can be digitized into Master Extension Sets, creating a portfolio of reusable libraries for environmental assets across carbon removal, emissions reduction, nature-based solutions, and emerging sustainability markets. As those libraries mature, they can help establish a more interoperable market infrastructure where buyers can compare credits with more confidence, registries can scale digital submission processes, and developers can access finance faster through trusted assets.

Impact Claim — Full Audit History

Claim History

#	Date	Status	Quantity	Updated By
3	2026-08-27 17:52	Completed	1.00	Verra Registry Agent
2	2026-08-27 17:36	Verified	1.00	DNV Simulation Admin
1	2026-08-27 17:35	Verification In Progress	1.00	1PointFive Simulation Admin

Checkpoints

Daily Checkpoint

2025-11-05 → 2025-11-05

Daily

2 tabs1 history

Checkpoint History

#	Date	EF Before	EF After	Updated By
1	2026-08-27 17:35	—	—	1PointFive Simulation Admin

Checkpoint Variables

QC02_nonVCS_injected_Ly

verra.ccs.extensionSet.QuantityOfNonVcsInjected

{ "InjectionPoint": "Shoe Bar ...

2 history

FFmass_x

verra.ccs.extensionSet.FlowMeterReading

{ "flowMeter": "DAC", "value": ...

2 history

#	Date	Data Type	Data	Updated By
2	2026-08-27 17:35	verra.ccs.extensionSet.FlowMeterReading	{ "flowMeter": "DAC", "value": 38851.97, "uOf": "tonnes" }	1PointFive Simulation Admin
1	2026-08-27 17:35	verra.ccs.extensionSet.FlowMeterReading	{ "flowMeter": "", "value": 0.0, "uOf": "tonnes" }	1PointFive Simulation Admin

Vn

verra.ccs.extensionSet.VerifyingEvent

{ "eventName": "none", "valu...

2 history

Monthly Checkpoint

2025-11-30 → 2025-11-30

Monthly

161 tabs1 history

Formulas

verra.ccs.extensionSet.modules.v0049_Formula3PercentCofMass

4 tabs1 history

The business case is therefore larger than a single release. Open sourcing the Verra CCS+ Master Extension Set converts hard-won implementation knowledge into shared infrastructure for the carbon market. It reduces duplicated effort, strengthens auditability, and gives market participants a practical way to move from document-based methodology interpretation to digital, automated, blockchain-enabled origination of high-integrity environmental credits.

You can get the Verra CCS+ Master Extension Set at

<https://github.com/VerraProjectHub/ccs-plus-extension-set>

The Verra Digital Gateway API Resources is available at

<https://projecthub.verra.org/digital-gateway-api>

SECTION VI

CONFIGURABLE INFRASTRUCTURE FOR ONCHAIN LENDING

WITH FOLKS FINANCE



PROBLEM BEING ADDRESSED

Onchain lending has consolidated into a small number of large pooled markets. In a pooled market, every listed asset draws on the same liquidity and is governed by a single shared risk configuration. That design made early lending markets possible, and it carries three consequences that have become limiting as the participant base has widened.

The first is that risk is collective. A single mispriced or thinly traded collateral asset can transmit losses to lenders who never chose exposure to it. The second is that parameters are collective. Interest-rate models, loan-to-value ratios, oracle selection and liquidation settings are set by protocol governance rather than by the institution bringing the assets. The third is that participation is open by default, with no mechanism to enforce identity checks, restrict counterparties or keep positions confidential.

For a regulated institution, the third point is not a preference but a condition of entry. An asset manager cannot lend into an environment where the counterparty set is unknown, and a bank cannot hold a position whose terms are subject to a governance vote it does not control.

The alternative available today is to build. An institution that requires its own parameters writes its own contracts, funds independent audits, staffs a permanent risk function and maintains its own interface. The cost is measured in quarters and in specialist hires, and it recurs with every change to the market design. Institutions are therefore left choosing between rails they do not control and a build they cannot justify. Most choose neither, and the credit that would have been extended is simply not extended.

The scale of unmet credit demand is not in dispute. The International Finance Corporation estimates the financing gap for formal micro, small and medium enterprises in developing countries at USD 5.2 trillion a year, affecting some 65 million businesses, with around 70 percent of such enterprises in emerging markets lacking adequate financing. Onchain infrastructure will not close a gap of that size on its own. But the institutions closest to that demand are rarely the ones able to fund a lending protocol from scratch, and the cost of building one is a barrier that has nothing to do with their willingness to lend.

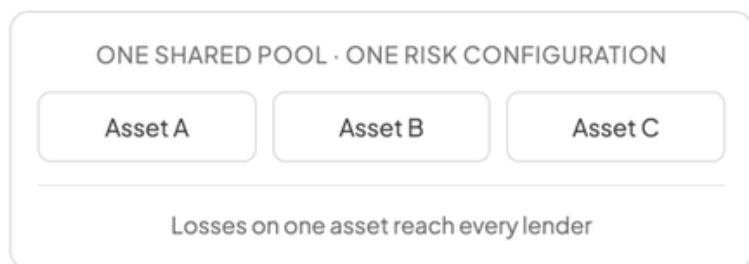
HOW THE SOLUTION WORKS

Onlend is a permissionless toolset for creating and running a lending application in as little as ten minutes, with no code required. A builder configures its own application and operates it, without writing smart contracts and without commissioning an audit of its own.

Each application is independent. It has its own collateral set, its own borrowable assets, its own interest-rate model, its own oracle, its own liquidation engine and its own access rules, and it is deployed under the builder's own brand and interface. Applications do not share liquidity, so the design intent is that a failure inside one is contained rather than propagated. They run on a shared contract core reused by every application deployed on it and subject to independent security review. Independent builders determine their own application's parameters, user access and regulatory requirements.

The configurable surface covers multi-collateral and multi-borrow markets; custom interest-rate models, including fixed rates, rates that track an external reference such as a staking yield, and targeted rates for defined groups of borrowers; any major oracle provider; a configurable liquidation engine; identity and whitelisting controls; deployment on a private network; a white-label front end; markets that are either updatable or permanently immutable; and analytics through REST and GraphQL interfaces.

POOLED ARCHITECTURE



MODULAR ARCHITECTURE



Figure 1. Pooled markets share liquidity and one risk configuration; modular applications share only the underlying contract code.

How it Leverages Blockchain

Four properties of blockchain settlement are what make this model work, and none of them has a straightforward equivalent in conventional infrastructure.

Shared Code with Separated State

Every application runs the same audited contracts while holding entirely separate balances and parameters. Reusing the code is what reduces deployment from quarters to minutes; separating the state is what makes the isolation real rather than administrative. Creating a lending market becomes a transaction instead of a software project.

Verifiability Without a Reporting Cycle

Collateral, debt, parameters, and liquidations are recorded publicly and can be checked continuously by lenders, borrowers, and auditors. A depositor is able to verify the solvency of the market they are lending into rather than being informed of it after the fact.

Enforcement as Code

Liquidations, rate rules, and access restrictions execute automatically and identically for every participant. Terms cannot be applied selectively, and no discretionary intervention is required to keep a market solvent.

Permissioning as a Setting

The same rail can operate as an open market or as a closed one with identity checks, whitelisted counterparties, and deployment on a private network. Regulated and public participants use one technology stack configured differently, instead of two parallel systems.

RESULTS AND LEARNINGS

Onlend's launch is targeted for the fourth quarter of 2026. The learnings below are what shaped the architecture: the constraints observed in existing pooled markets, and the requirements institutions set out when evaluating the infrastructure.

Risk containment has to be structural

In a pooled market, the only meaningful lever on risk is what gets listed, and every listing decision is taken on behalf of all lenders. Conservative listing keeps losses low but sets the ceiling low too: assets that could be supported safely in isolation are declined because they cannot be supported safely alongside everything else. Isolation moves that decision to whoever carries the exposure.

Isolation widens what can be lent against

Once an application cannot transmit losses to any other, collateral that no shared pool would accept becomes viable: tokenised real-world assets, long-tail collateral, assets with thin secondary liquidity. The constraint shifts from what the wider market will tolerate to what the builder is prepared to underwrite.

Institutional participation stops at permissioning

For regulated counterparties the recurring obstacle is rarely yield or asset coverage. It is the absence of identity checks, counterparty whitelists, and confidentiality. These are prerequisites, and a market that cannot express them is not a candidate regardless of its other properties.

Configuration is the product

Institutions that want a market of their own are generally not short of appetite or of assets. They are short of engineering capacity and audit budget. Removing that requirement, rather than adding features to a shared pool, is what turns intent into a deployed market.

FUTURE OPPORTUNITIES

The applications expected first after launch are:

- **Real-world asset lending.** Credit against tokenised treasuries, funds, and private credit, with identity checks applied at the application level.
- **Leverage on yield-bearing assets.** Issuers of staking and yield-bearing tokens offering leverage on their own asset, under their own brand.
- **Fixed-rate, fixed-duration credit.** Terms that resemble conventional lending agreements more closely than variable pool rates.
- **Consumer credit inside existing applications.** Wallets and digital banking applications extending credit against collateral their users already hold.
- **Permissioned and private deployments.** Applications on private networks for institutions whose obligations preclude a public one.

Allocation vaults, which route deposits across applications, are planned separately after launch.

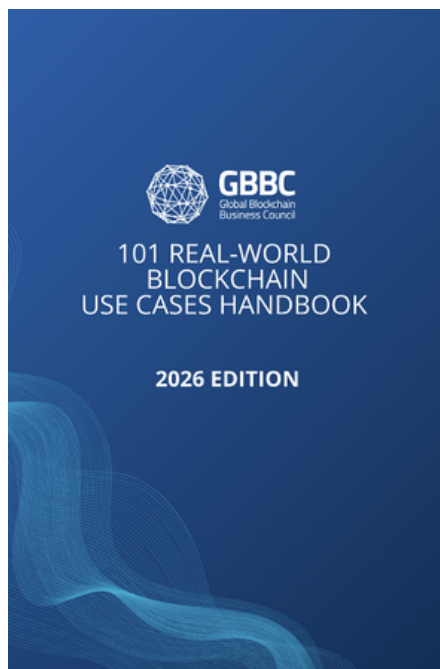
The longer-term opportunity is a change in who is able to operate a credit market. Establishing one has historically required either a balance sheet and a licence or a full engineering organisation. If the cost of a compliant, risk-isolated lending application falls to a configuration exercise, the set of institutions able to extend credit widens to include regional banks, cooperatives, fintechs, and asset managers in markets where the infrastructure to do so has never been locally available. Access to credit sits behind both the first and the tenth United Nations Sustainable Development Goals, and lowering the cost of building the infrastructure is one contribution to it.

CONCLUSION

Onchain lending demonstrated that credit markets can settle transparently and enforce their own terms. What it did not resolve is who gets to set those terms. Onlend addresses that question by treating a lending market as something an institution configures rather than something it either accepts as given or builds from nothing. The first applications are targeted to go live in the fourth quarter of 2026, subject to testing and independent security review.

101 Real-World Blockchain Use Cases Handbook

In 2026, GBBC released the second edition of the *101 Real-World Blockchain Use Cases Handbook*, a valuable reference guide for government agencies, regulators, and central banks worldwide to deepen understanding of blockchain and digital assets.



Access the digital version using the QR code:



To submit a use case for consideration in 2027, complete the form below*:



**Priority given to GBBC members*

