Exploring Blockchain

FOR DISBURSEMENT TRACEABILITY

Outcome Report
November 2020

Technology & Innovation Lab

WORLD BANK GROUP
Finance & Accounting

Abstract

The World Bank Finance and Accounting (WFA) VPU and the World Bank Technology and Innovation lab (ITSTI) embarked on journey to learn how Blockchain could enhance the loan disbursement traceability process. This outcome report shares the key learnings and insights as a part of the internal and external exploration.

Acknowledgements

This initiative was made possible by the collective effort of World Bank Group staff from the World Bank Finance and Accounting and Information and Technology departments, and the participation and guidance received from colleagues in the Legal and Corporate Procurement. The key learnings outlined in this report were prepared by the Blockchain For Loan Disbursement Traceability project team.

World Bank Finance and Accounting (WFA)
Michael Ochieng, Junxue Chu, Jayavishnu Babu Nattanmai Subburamiyer Jayaraman, David Liow, Victor Ordonez

Information Technology Solution, Technology and Innovation Lab (ITSTI)
Yusuf Karacaoglu, Stela Mocan, Mahesh Chandrahas Karajgi, Raunak Mittal, Emmanuel Crown, Rachel Alexandra Halsema, Mora Farhad

Information Technology Solutions, Finance (ITSFI)
Valentin Prudius, Pascal Platteborse, Ramraj Rangarajan and Atul Gupte

Information Technology Solutions, Risk and Compliance (ITSSR)
Zhijun William Zhang

Legal Counsel (LEG)
David Satola, Patricia Miranda

Corporate Procurement (SPACP)
Sanjay Colaco, Shweta Mesipam

Contents

Executive Summary

The effective monitoring and evaluation of projects funded by the World Bank (WB) funded is a challenging and time-consuming process. Currently, stakeholders involved in World Bank funded projects use separate financial management systems to trace payments and keep records, meeting stakeholders' requests for records can be a difficult process. The work involved in coordinating the activities of several teams within the World Bank and Project Implementation Units (PIUs) is a labor-intensive task. **The World Bank Finance & Accounting (WFA) in collaboration with the World Bank Group/ITS Technology Innovation Lab (the project team) worked on a challenge framing exercise to prototype a solution that addresses these challenges.** The project team, in its journey to identify the best suitable technology, explored the use of blockchain as a potential technology solution. Transactions, records and digital assets stored on a blockchain platform are immutable, permanent, secured, and shareable; these key blockchain functionalities will enable the World Bank, its member countries, and its Borrowers to have "one version of truth" during the lifecycle of World Bank funded development projects.

In looking for a solution to the disbursement traceability challenge, the World Bank aimed to acquire a technology that can be scaled easily to accommodate over 3,000 active projects, as well as to enable multiple external parties to participate, and ensure that the many existing World Bank systems could potentially be integrated into the solution. As an emerging technology, blockchain is undergoing constant change; the World Bank is interested in a solution that could survive any major changes within the blockchain ecosystem within the next few years and be interoperable to allow flexibility.

The World Bank project team developed an in-house prototype and validated the suitability of blockchain technology for the disbursement traceability challenge, and assessed the viability of building a blockchain platform that is agnostic to WB-funded development projects. The transformative potential of Distributed Ledger Technology (DLT) and Blockchain has generated interest to better understand what is currently available in the commercial marketplace. As a result, the project team launched a request for an expression of interest (REOI) in February 2020. The external exploration was highly successful and attracted 79 solicitations, 22 of which were shortlisted, with four technology partners making the final selection. These partners included Ernst & Young (EY), cLabs (CELO), Securrency and Stellar Development Foundation (SDF), and Orbs and Matrix. In the spirit of learning and collaboration, the four technology partners worked independently to assess the business challenge, and each built a functional prototype to demonstrate the capabilities of their respective solutions.

The requirements set forth in the REOI emphasized the importance of security, data privacy, scalability, maturity, and interoperability. In addition, key questions were asked as to who would own and operate the platform, what the cost estimates were, and what the options were for implementation. This report highlights the exploration journey of experimenting with Blockchain/DLT, and aims to share the learnings and knowledge across the WBG and the international community.

Introduction

The World Bank, through its WBG/ITS Technology and Innovation Lab, experimented with open source Blockchain and DLT protocols to address the disbursement traceability challenge in on-going Bank projects. The preliminary findings from the Lab prototyping ("Phase A") were found to be positive; however, further exploration and field testing will be needed before the technology could potentially be adopted at the enterprise level.

In Phase B, the project team launched a REOI and partnered with four technology partners with proven track records of advanced experimentation with Blockchain and DLT for the traceability of funds. Recognizing that engagement with any single technology partner poses risks because of the pace of technological changes, and to facilitate an inclusive and participatory learning process, Phase B results will be shared with the public via online repositories (e.g. GitHub) and during knowledge-sharing sessions.

Phases A and B entailed an in-depth exploration of various business and disbursement scenarios and the different available models of Blockchain/DLT technology to enhance the traceability and accountability of funds. This report aims to share the approach and knowledge gained through the internal and external phases of the project, including the risk and implementation considerations for a production-ready system and the building blocks needed to build a minimal viable product (MVP).

Background

1.1 Project Background

The World Bank is the world's largest source of funding and knowledge on development solutions. It uses its financial resources and extensive experience to help client countries reduce poverty, increase economic growth, and improve quality of life. It is governed by 189 member countries and delivers services out of 120 offices, and employs 16,000 staff globally.

The World Bank Finance & Accounting (WFA) Vice Presidential Unit is responsible for all aspects of the financial reporting and internal control framework of the International Bank for Reconstruction and Development (IBRD), the International Development Association (IDA), and the extensive Trust Fund/Partnership portfolio of these entities. WFA also leads the client shared service function for the World Bank's corporate expenses and its trust funds, and ensures fiduciary responsibility for all disbursements related to Bank operations; it is also responsible for disbursements involving about 3,000 active projects financed annually by the World Bank.

One of the World Bank's key mandates is to ensure that the funds deployed to finance development projects are being used for their intended purpose. An increasing number of member countries and large donors have begun to approach the World Bank with requests for documentary proof, e.g. procurement contracts, invoices and proof of payment of disbursement transactions, to ascertain whether the funds they have donated are being used properly.

Currently, the World Bank uses internal systems to disburse and monitor funds disbursed to Borrowers or PIU countries. Once funds are released for projects, WFA has full traceability and disbursement documentation available; however, it has limited traceability on how funds are used and which participants are being paid after these funds are released, as most projects have multiple layers of participants (e.g. intermediary agencies, suppliers, NGOs, etc.) that receive funds before they reach end beneficiaries. Ultimately, Borrowers/PIUs have the responsibility to keep track of how the funds are used and retain original documents of eligible expenditures, and making them available for audit or inspection. However, the World Bank does not ask for copies of all original documents for the many projects it is responsible for; instead, Borrowers/PIUs can submit summary expenditures reports in the form of interim unaudited financial reports or expenditure statements, which summarize eligible expenditures paid over a given period.

Many challenges present themselves when member countries and donors submit requests to obtain relevant records to review projects and transactions. In most cases, storage of hard copies of receipts and records are only accessible by Borrowers/PIU members; in addition, they may be stored in multiple locations, and may be difficult to obtain once a project is completed. These review requests by member countries and donors are often extremely labor intensive for both the World Bank and Borrowers/PIUs.

1.2 Loan Disbursement and Traceability Challenge

The World Bank's Finance and Accounting Vice Presidency approached the WBG/ITS Technology and Innovation Lab to help tackle the disbursement traceability challenge.

The current disbursement process between the World Bank and PIUs (e.g. national governments) relies on the WB Client Connection system. Under this process, the World Bank does not keep records of stakeholders further down the disbursement value chain. **Once the Bank disburses funds, PIUs have responsibility over the management of these funds, as well as maintaining records of eligible payments to suppliers, intermediary or citizens.** Three main challenges must be overcome to achieve end-to-end disbursement traceability in an efficient and effective manner:

This process presents three main challenges:

- Currently, the storage of records which could facilitate the traceability of disbursed funds is principally only accessible to PIUs, and usually only in hard copies which makes it difficult to obtain these records;
- It is difficult to obtain records if recipient PIUs close after project completion; and
- Labor intense coordination efforts are needed to obtain records requested by auditors.

TWO

Blockchain Exploration

Blockchain Exploration

2.1 Exploration with Blockchain and DLT

The World Bank Information & Technologies Solutions (ITS) created the Technology & Innovation Lab (ITSTI) to provide a learning platform, exploration space, and provide technology advice on disruptive technologies. The ITSTI team collaborates and partners with ITS counterparts, internal WBG business units, and external stakeholders to explore, test and understand new technology capabilities to enable the WBG to fully harness the Digital Age. To achieve its mission, ITSTI engages and partners with leading technology companies and start-ups, entrepreneurs, innovators and development organizations to experiment, develop and roll out Blockchain-enabled solutions. This initiative aims to bring together development practitioners and facilitate learning efforts across the WBG on DLT and Blockchain. Additionally, ITSTI strives to improve the organization's capability to embrace innovation in internal operations, and to respond to inquiries and needs from client countries.

The approach taken by ITSTI consisted of:

- Experimenting and exploring by developing use cases focused on specific problems, leveraging collaboration with external experts, thought leaders and technology partners to develop our knowledge, skills and expertise in the DLT space.
- Learning through Proofs of Value (PoV) use cases on the potential benefits of Blockchain in addressing and solving development challenges.

2.2 Blockchain For Disbursement and Traceability Challenge

The current disbursement process between the World Bank and PIUs (i.e. national governments) uses the World Bank’s Client Connection system. This process does not require the World Bank to keep records of stakeholders further down the disbursement value chain. Once funds are disbursed to PIUs, they are responsible for managing the funds, and keeping records of eligible payments to suppliers, intermediary or citizens.

The World Bank’s Client Connection system is accessible to users around the world. This creates opportunities for cyberattacks, leading the team to make considerable efforts to secure the Client Connection system. However, as new threats emerge, the system could become vulnerable. However, if the DApp approach is adopted, each blockchain node could only be potentially accessed by “local” users through their associated DApp, which would most likely decrease its vulnerability to cyberattacks.

Currently, the integrity of data in the Client Connection system relies on a database maintained by the World Bank. A rogue DBA in the World Bank could change the data. With a distributed ledger solution, each change to data, triggered by either a direct value transfer request or the execution of a smart contract, would require a consensus process among the validator nodes. Under this scenario, data integrity would be strengthened as it is maintained by all validator nodes.

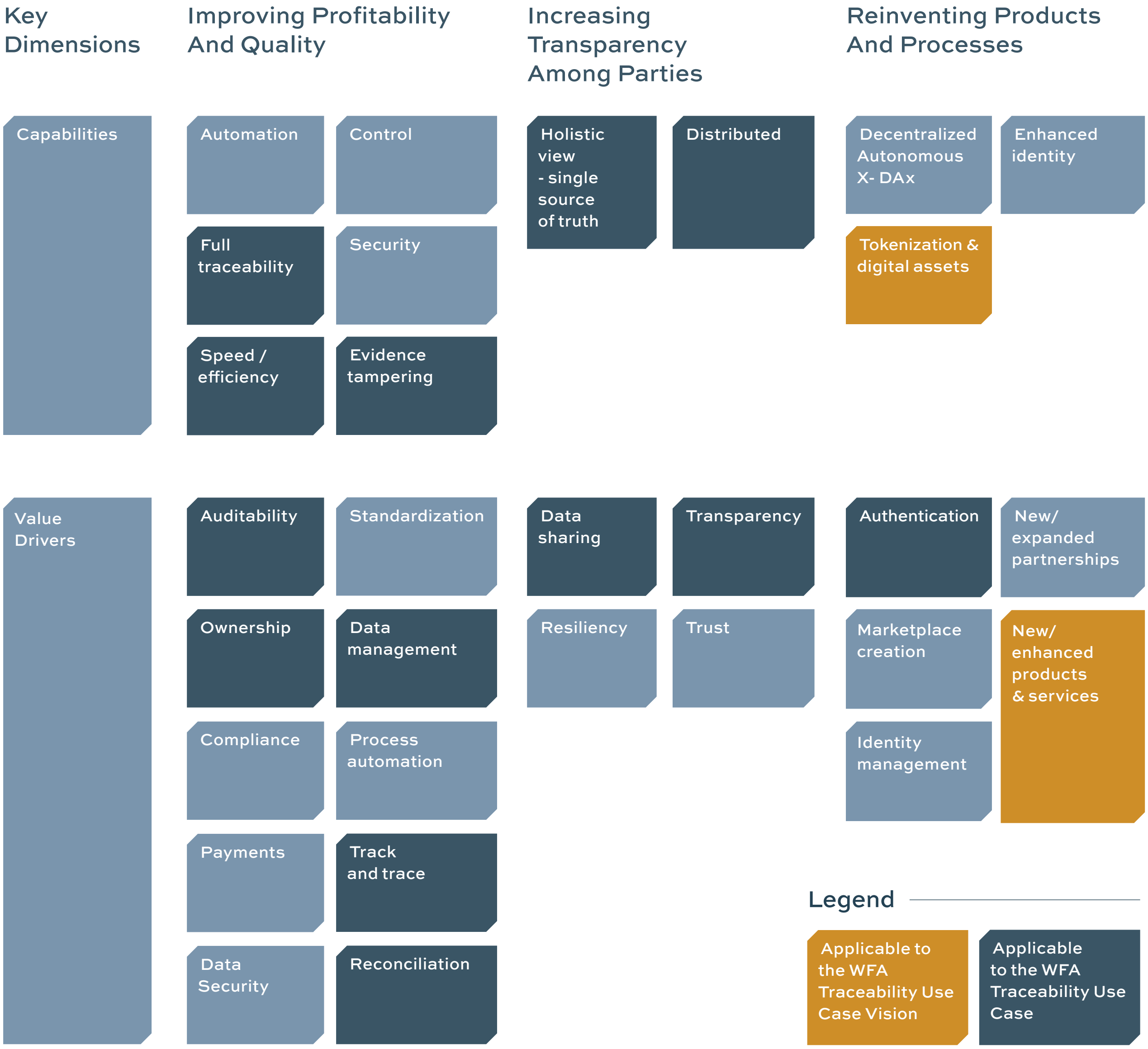
Why Blockchain?
Why Not Client Connection?

	Challenge With Client Connection	How Can Blockchain Address This?
Security	Providing global access to an internal WB financial system induces security threats.	Designed for a distributed and secure access to business process networks. No single point of failure
Data Ownership	WB will need to maintain ownership of client data.	Clients countries can own their data.
Tokenization	Not possible to implement digital tokens of digital assets.	Provides the core ability to implement digital tokens. and digital assets.
Immutability	Reliability of data questionable due to centralized control.	Secure, auditable and immutable data capture through unprecedented shared control.
Scalability	Not feasible to scale up accomodating project variations limiting network expansion.	Allows us to create a permissioned multi organizational network and scale on demand.

The World Economic Forum (WEF) developed the framework below to evaluate the potential benefits of Blockchain for specific solutions. The framework depicts the benefits of using Blockchain technology for the WFA traceability project. The dark blue squares show the value applicable to the prototype being built to support the activity. The light blue squares represent the potential long-term value if the technology is scaled up by the World Bank. Descriptions of each relevant capability and value driver are listed below.

WEF & Blockchain

Value Framework for WFA Traceability



Key Dimensions	Improving Profitability And Quality	Increasing Transparency Among Parties	Reinventing Products And Processes
Capabilities	Automation Control Full traceability Security Speed / efficiency Evidence tampering	Holistic view - single source of truth Distributed	Decentralized Autonomous X- DAx Enhanced identity Tokenization & digital assets
Value Drivers	Auditability Standardization Ownership Data management Compliance Process automation Payments Track and trace Data Security Reconciliation	Data sharing Transparency Resiliency Trust	Authentication New/ expanded partnerships Marketplace creation New/ enhanced products & services Identity management

Legend

Applicable to the WFA Traceability Use Case Vision

Applicable to the WFA Traceability Use Case

Capabilities

1. **Full Traceability:** The World Bank and key stakeholders can track and trace end-to-end transactions to retrieve project documents and expenditures.
2. **Evidence Tampering:** No records are deleted. Any data manipulation, e.g. a status change that makes no logical sense, can be traced and corrected by the relevant partner organization.
3. **Speed/ Efficiency:** Documents and expenditure data are readily available to stakeholders on this platform.
4. **Holistic View/Single 'Source of Truth':** A single 'source of trust' and reliability is established if entities use the platform consistently for every transaction.
5. **Distributed:** Distributed ledgers cut down on operational inefficiencies by providing a reliable platform for all transactions and maintaining data privacy.

Value Drivers

1. **Auditability:** Transactions are immutable: once written, they cannot be modified or deleted.
2. **Ownership:** More than one entity can write or read the database. Access may be permission-less (i.e. public) or permissioned (i.e. private).
3. **Data Management:** A shared platform to keep an organized, transparent and traceable collection of data to benefit all relevant stakeholders.
4. **Track and Trace:** The capability to track the inflow to outflow of data.
5. **Data Sharing:** Provides a structured repository of information between parties involved in a project or transaction.
6. **Transparency:** The data and documentary evidence captured are permanent and available to all parties involved in the transaction, while also maintaining data privacy.
7. **Authentication:** Participants have a digital identity in every transaction.

2.3 Business Challenge Scope

The World Bank Finance & Accounting (WFA) in collaboration with the World Bank Technology & Innovation Lab ("WB project team") worked on a challenge framing exercise to develop a solution that addresses these challenges described as "Phase A". The solution had to be universally applicable to facilitate tracking and tracing of funds disbursed to any type of WB funded development projects as captured by the identified disbursement scenarios.

The WB project team in its journey to identify the best suitable technology, explored the use of DLT and Blockchain as a potential technology solution. Transactions, records, and digital assets stored in the blockchain platform are immutable, permanent, secured, and shared – key blockchain functionalities that will enable the World Bank Group, its member countries, and its borrowers to have "one version of truth", during the life-cycle of implementing development projects funded by the Bank.

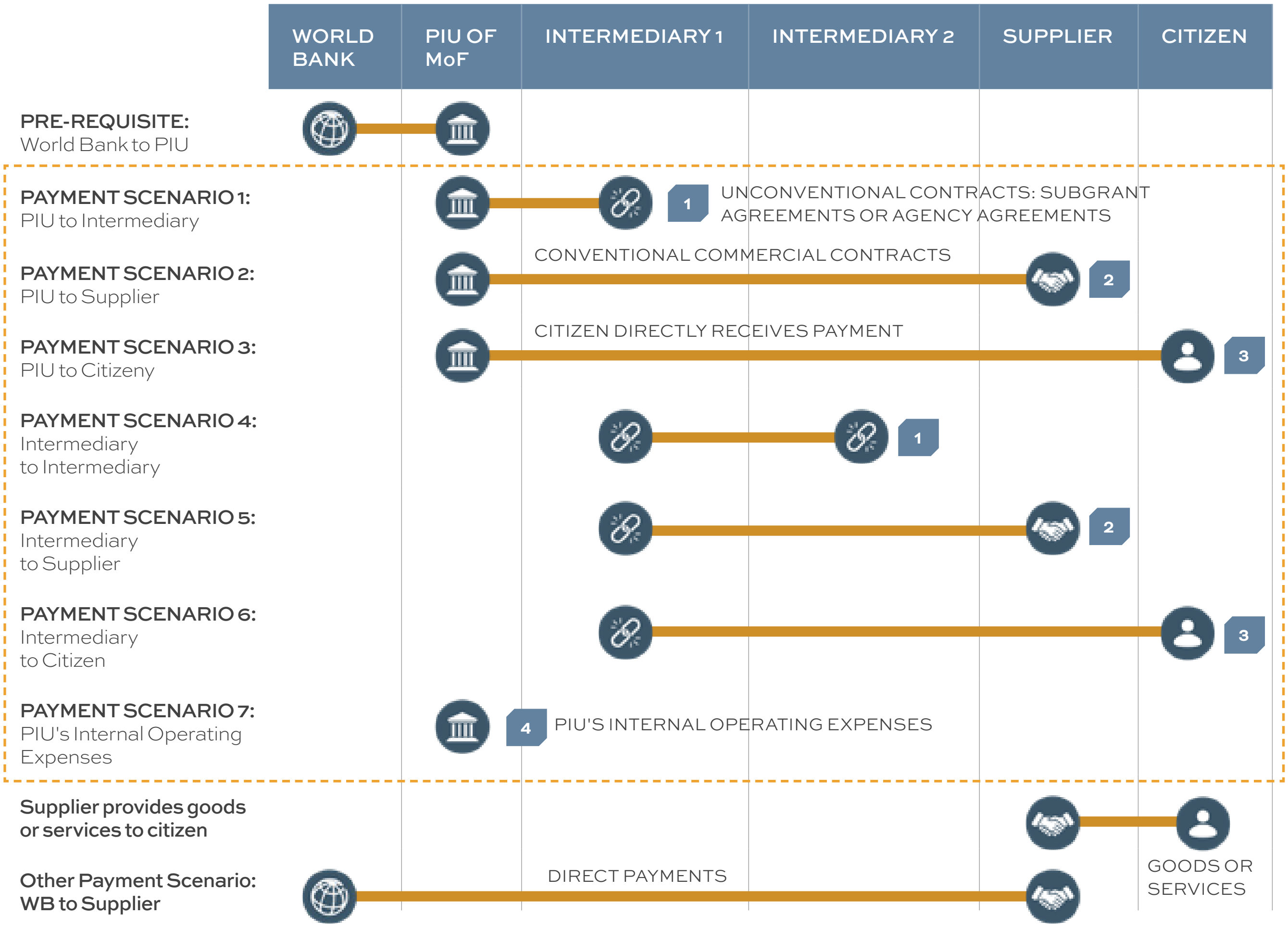
At the core of a DLT and Blockchain solution is a trusted common and shared system platform in which all parties involved in development projects are implicated. This system platform would:

i. Facilitate collaborative project implementation;
ii. Enhance traceability of how the funds are expended;
iii. Provide self-servicing capabilities;
iv. Facilitate transparency throughout project implementation;
v. Offer near real-time access of records to all interested parties;
vi. Ensure the permanence of records uploaded to resolve inactive PIU scenarios; and
vii. Provide a capability to perform KYC and AML checks.

2.4 Business Process and Disbursement Scenarios

Over a series of meetings and workshops, the project team mapped the World Bank's current disbursements processes. The figure below highlights the majority of the World Bank's current disbursement scenarios.

TRACEABILITY SCENARIOS ACROSS ACTORS BEYOND RECIPIENT (PIU)


WORLD BANK
PIU OF MoF
INTERMEDIARY 1
INTERMEDIARY 2
SUPPLIER
CITIZEN
PRE-REQUISITE: World Bank to PIU
PAYMENT SCENARIO 1: PIU to Intermediary
1
UNCONVENTIONAL CONTRACTS: SUBGRANT AGREEMENTS OR AGENCY AGREEMENTS
PAYMENT SCENARIO 2: PIU to Supplier
CONVENTIONAL COMMERCIAL CONTRACTS
2
PAYMENT SCENARIO 3: PIU to Citizeny
CITIZEN DIRECTLY RECEIVES PAYMENT
3
PAYMENT SCENARIO 4: Intermediary to Intermediary
1
PAYMENT SCENARIO 5: Intermediary to Supplier
2
PAYMENT SCENARIO 6: Intermediary to Citizen
3
PAYMENT SCENARIO 7: PIU's Internal Operating Expenses
4
PIU'S INTERNAL OPERATING EXPENSES
Supplier provides goods or services to citizen
GOODS OR SERVICES
Other Payment Scenario: WB to Supplier
DIRECT PAYMENTS

2.5 Phase A: Internal Lab Prototype and Outcome

As an outcome of this initial phase, the team concluded that challenges could be tackled by building a shared and common technology platform connecting all stakeholders involved in the implementation of development projects.

The team used Azure Blockchain as a service, on-cloud storage and Power BI to prototype the core features of the solution. The system consists of Blockchain nodes owned by some stakeholders, which gives them their own copy of the project implementation data. The prototype enabled the team to validate the suitability of blockchain technology for the disbursement traceability challenge, and assess the viability of building a Blockchain platform that is agnostic to WB-funded development projects. The team concluded that the design pattern of an off-chain database can offer a richer analytics experience for stakeholders, e.g. the World Bank's management team, donors and shareholders. Furthermore, the Blockchain solution can be scaled up and used to facilitate tokenization which enables the flow of funds to be tracked from end-to-end, i.e. from inflow to outflow, until it reaches the intended purpose. Additionally, the solution can be integrated with the World Bank or recipient countries' systems. However, the development of this solution was solely intended to serve as a testing and exploration opportunity to assess the use of Blockchain and DLT in addressing the business challenge; however, the developed prototype is not production-ready in its current form. The success of the World Bank's prototype garnered interest from industry leaders as they seek to further explore the feasibility and challenges of operationalizing a production-ready Blockchain system to enhance transparency in disbursed funds.

2.6 Phase B: Learning Objectives and Scope of Proof of Concept (PoC)

Phase B of the project extended the exploration through a PoC to assess the suitability of Blockchain and DLT open-source solutions for enterprise adoption. In this phase, PoC activities were meant to define the business logic, design patterns, implementation framework, costing, and country context considerations in order to inform a pilot, production-ready solution. The project team recognized that the pace of technological change precluded opting for a single technology partner, and decided to partner with up to four partners with a proven track record of experience with Blockchain and DLT for the traceability of funds. To facilitate an inclusive and participatory learning process, the learnings from this phase will be made public via online repositories (e.g. Github), as well as in the course of knowledge-sharing sessions with international communities.

Phase B Deliverables: The shared deliverables from the PoC included:

- Technical documentation of potential solution architectures;
- Design patterns or ideas related to document storage, privacy, and scalability;
- Source code (e.g. front-end, APIs, smart contracts);
- DLT protocol, to be made available as open source;
- Instructions and files necessary to set up the prototype for testing;
- Limitations to the proposed solution; and
- Questions and clarifications raised by the World Bank and technology partner

2.7 Phase B: About the Technology Partners

The REOI attracted 79 solicitations from technology firms. The evaluation committee comprised colleagues from the WFA business teams, the Technology and Innovation Lab, the ITS Finance complex, and the Security and Information teams. Twenty-two proposed were shortlisted, and four technology partners were included in the final list. One of the preconditions of the evaluation criteria was that the selected technology firms must have proven experience in delivering a production-ready DLT system which incorporates security, data privacy, scalability, and is interoperable. The proposals needed to demonstrate whether the proposed solution could address identified challenges and achieve the business objectives of traceability of loan disbursements made by the World Bank.

Technology partners were expected to address the following key questions in their proposals:

TECHNOLOGY PARTNER	CITY, COUNTRY	KEY STRENGTHS
Ersnt & Young	New York, US Toronto, CA	Large and well experienced Blockchain team, EY OpsChain platform, ERP integration, Privacy and Scalability, and Analytics
C-Labs	San Francisco, US	Celo platform, mobile driven and widely accessible. User onboarding solution & experience, UXM and thin mobile layer benefits FCV countries
Securrency (along with SDF)	Annapolis, US Abu Dhabi, UAE (San Francisco, US)	Securrency has extensive experience in the Financial Sector with focus on compliance, policy enforcement, and tracking of founds flow. SDF is a major industry player focused on real-time cross border payments with strong technology and human talent
ORBS (along with Matrix)	Tel Aviv, IL Singapore, SG	Public blockchain infrastructure and support permissioned apps. Unique blockchain technology architecture, such as V-Chain.

KEY AREA	KEY QUESTIONS
Feasibility	Is blockchain the best technology solution for our challenge and use case?
Scalability	Can the system potentially scale to accommodate the 3000+ WB projects and participants?
Interoperability	Can the system integrate with existing WB and Borrower system & other blockchain platforms?
Data Privacy	How does the blockchain ensure data privacy?
Implementation Options	What are the available potential options?
Ownership	Who will own, operate, and maintain the platform?
Cost	How much would a production system cost?

CLabs

cLabs built a prototype solution on the Baklava Test net, a staging network for the Celo public blockchain. The solution leverages Web technologies, including traditional relational datastores to store documents and user information, and uses the Celo blockchain to "notarize" documents by storing a cryptographic hash on the blockchain instead of the full document. The use of tokens is supported in the solution but is not currently employed. The Celo Main net is an open and public blockchain network, but a permissioned (i.e. private) network is also possible on Celo.

SDF and Securrency

The solution proposed by SDF and Securrency is built on the Stellar public blockchain, and adopts a unique approach which focuses on incorporating tokens and transfer of value on the blockchain. Although the prototype can track and trace without the on-chain transfer of value, this technology firm emphasized the point that the use of blockchain without a corresponding on-chain transfer of value significantly limits the advantages of blockchain. The automation of business processes and compliance (i.e. policy enforcement) substantially enhances efficiency when embedded in the token representing the actual value being transferred. The prototype has four unique interfaces to meet the needs of all participants and includes a mobile wallet. The prototype can be run on a public or private ledger, but Securrency and SDF have recommended the use of public ledgers for speed, security, and most importantly, increasing global access.

Orbs and Matrix

Orbs created a solution on the Orbs blockchain which leverages the platform's unique virtual chains (vChains) and Secure Messaging Infrastructure (SMI). vChains provide an isolated set of computational resources to an application consisting of SMI running on one such vChain operated by all nodes, and project-specific applications running on dedicated vChains operated by subsets of the nodes deployed to the network participants. The SMI allows the encryption of messages to a defined set of recipients, with only the intended recipients able to decrypt the message. The Orbs blockchain can support a solution with permissioned (i.e. private), or permission-less (i.e. public) blockchain. The public blockchain is secured and supported by the Orbs Proof-of Stake ecosystem. Orbs' solution did not employ tokens as the focus of the challenge was traceability but the solution can support tokens and transfer of value when needed.

EY

EY's solution is created on EY OpsChain, which is a proprietary platform and open-source Ethereum blockchain protocol. It also has foundational open-source software components (e.g. Nightfall and Baseline protocols, smart contract templates, tokenization, Blockchain analyzer), which could allow the World Bank and stakeholders to interact with each other in a secure manner either through a private or public blockchain, thereby protecting privacy.

THREE

Outcome and Learnings

Outcome and Learnings

3.1 World Bank Loan Disbursement Traceability Key Learnings

Platform Ownership, Nodes:

Solutions are usually built on public or private blockchains, but ownership of the platform can vary depending on the operating model. Technology partners reiterated that the goal would be to have an open source, decentralized platform, with shared ownership among stakeholders.

However, if a Blockchain solution was to be pursued, the World Bank would initially be the main stakeholder and maintain ownership of all governance rights and authority over the nodes being operated. The World Bank would "own" the platform and bear the initial set-up costs. The selected Blockchain vendor would be responsible for the maintenance of the platform and system.

Most technology partners suggested that between 6-11 nodes would be needed for the 5-7 pilot projects. The World Bank would operate the nodes initially, and thereafter progressively decentralize and allow other trusted parties to begin running their own nodes on a case-by-case basis. Other trusted entities running nodes could be government ministries, UN agencies, donors, or suppliers/intermediaries.

3.2 Solution Design Architecture Learnings

KYC/AML

Business Context: As a specialized agency within the UN family of organizations, the World Bank pays due regard to decisions of the UN Security Council under Chapter VII of the UN Charter, and it is World Bank's policy not to make payments to persons or entities listed on the UN sanctions list. The Bank is also required under its Articles to "make arrangements to ensure that the proceeds of any loan are used only for the purposes for which the loan was granted . . . without regard to political or other non-economic influences or considerations."

The World Bank performs "Know your Customer" (KYC) and "Anti-money Laundering" (AML) checks on all parties it pays directly, including lendors, banks, donors, recipients and World Bank employees. Furthermore, it relies on MoF/PIU counterparts to run checks on other parties involved in a project, which the Bank does not have a direct payment relationship with. It is therefore important to incorporate KYC/AML elements when registering blockchain participants to ensure that the Bank adheres to requirements under its Articles.

Applicability: The disbursement traceability project for WB-funded projects involves various stakeholders and participants, ranging from PIUs to intermediaries, suppliers (contractors and subcontractors), and beneficiaries. To leverage DLT/blockchain technology for the traceability of funds, these different participants would need to interact with the proposed technology platform. To ensure the security and legitimacy of participants, the project team sought to address concerns relating to the KYC and AML capabilities outlined below. Before the World Bank is able to collaborate with client countries or PIUs and set up a technology platform, or even become a participant in a disbursement traceability platform, it will need to understand:

- What are the liability concerns or reputational risks around KYC/AML that World Bank should be aware of?
- Who would be responsible and bear the onus of performing KYC/AML checks?
- How the World Bank could gain confidence and be assured that participants are appropriately KYC'd?
- How would the KYC/AML take place which can be proposed to the appropriate stakeholders as best practices?

Key Learnings and Proposed Approaches: Although the project team acquired valuable insights and learnings in the course of this exploration phase with technical partners, more clarity and scope for further work is needed on the topic of KYC/AML. The learnings were either through some demonstration on the prototypes, or through various knowledge exchanges and technical deep dives between the project team and technical partners.

It is important to note that some KYC/AML requirements and corresponding approaches would vary according to the solution design. For instance, if an on-chain transfer of value is explored, it would be accompanied with additional requirements, as well as policy and compliance-related issues. However, irrespective of the chosen approach, the team was able to obtain a number of key insights on applicable KYC/verification and AML practices, both at the institutional level (WB), downstream entities (PIUs) to the end-beneficiary and citizen level:

- The initial anticipation is that the KYC process would not undergo many changes from the proposed solution of using blockchain for traceability, and the respective parties in the disbursement chain would continue to perform existing KYC/AML processes. The process could continue to take place off-chain, as currently happens, with the possible integration to the envisioned solution platform.
- As per functional requirements, all the relevant parties that need to be KYC'd would need to submit the required documentation during the on-boarding process. This would be vetted by the intended actors and the verification documents would then be notarized with its hash on the blockchain. The KYC'd documents themselves would be off-chain. Proof of the verification would remain on-chain for other relevant parties to query and verify, without revealing the underlying information.
- Integration to the existing KYC/AML systems of participating parties, for example Lexis/Nexis in case of the World Bank, could help them achieve higher automation levels in the KYC/AML process.
- Additional considerations are required for KYC in the scenario where the solution design leverages tokenization for disbursements and traceability. In such a case, a third-party digital wallet provider, or an intermediary responsible for on-boarding participants on the network, would be responsible for performing KYC, as per the applicable criteria.

- Various AML capabilities and fraud detection analytics can be integrated in the proposed platform. Strong desirable AML capabilities could be achieved through smart-contract enabled fraud detection; this could be done by programming in a series of requirements and blockchain analytics tool to monitor the flow of funds on the blockchain. This could potentially help to ensure that funds can only flow between approved participants, as well as flag any suspicious activities with any account/wallet for the payee to take appropriate action.

Data Privacy and Security

Business Context: The World Bank stresses the importance of data privacy and security when working on projects. Not only does the Bank have its own standards to meet for data privacy, but when funding projects using trust funds, routine audits are performed to make sure that the procedures used in the project adhere to the privacy standards of member states. Any solution and system that the World Bank uses must be secure and able to adhere to stringent data privacy standards.

Different technology partners have proposed different approaches to support transaction privacy. However, all platforms support the recording of hash values of supporting documents associated with the transactions, so that no actual document data will be recorded on the blockchain.

For solutions based on a public blockchain, some technology partners have proposed to use a virtual chain approach to restrict which network nodes can participate in private transactions. Other partners would rely on zero-knowledge proofs (ZKPs) to provide transaction privacy, even though this technology has not been fully implemented on all platforms.

For solutions based on a private blockchain, besides restricting membership on the network, the use of smart contracts has been proposed to provide fine-grained access control on transaction execution, with the use of ZKP to provide data confidentiality.

Identity and Access Management

Identity and access management for a blockchain network need to operate at both the node level and the user level. At the node level, the identity of a node can be used to determine whether this node can participate in a permissioned network. At the user level, a user typically participates in the blockchain network's activities using a wallet, in which a private key is stored and used to sign transactions or claim ownership of digital assets.

In our POC, both levels of identity and access management have been employed. In addition, some solutions have provided a traditional application in which users can use a traditional Web identity to authenticate themselves and gain access to the application. In the case of traditional Web or mobile application and to achieve true data integrity and non-repudiation of the transactions, this may still require the end user to use a digital wallet to sign transactions or documents.

Some technology partners considered the need of users who do not have a smartphone, and developed a solution for users with feature phones to sign transactions. Others introduced KYC/AML checks as an integral part of the identity system, so that only verified users can participate in transactions that have compliance requirements.

Moving to a Distributed System: Security and Risk Implications

A blockchain-based solution inherently has a distributed architecture. With this new architecture, we will be shifting some, if not all, external users from accessing World Bank's systems directly at the UI layer, to a new model in which users will access their own user interface; this, in turn, will trigger transactions that are populated from their blockchain node to other nodes on the blockchain network.

Such a distributed architecture should increase the user's community level of trust in the system, as data integrity is maintained by the whole community, and also because multiple copies of the same data could be used for validation. One security issue with this model is whether all the nodes of the blockchain network can be maintained as securely as the World Bank would do. However, given the availability of cloud computing across the world, it is feasible for a secure configuration to be defined and validated so that participating organizations can run their own nodes without compromising the security of the overall network.

Another potential risk area is the rigor in user on-boarding and lifecycle management. This can be addressed by establishing standard requirements for user on-boarding and leveraging a network of trusted authorities to issue verifiable claims of user identities, so that no matter which node a user would connect to, the same validation process is followed, with proofs available for identity verification.

3.3 Feasibility, Interoperability, Maturity, and Scalability

The following discussion is limited to the 'tracking and tracing functionality' and does not cover the future scenario where a blockchain could be used to support the exchange of value.

Any production grade solution implemented to capture the evidence related to eligible payments, e.g. to suppliers, intermediary or citizens, will only serve its main intended purpose (i.e. to obtain the relevant records any time in future) if the following two main conditions are satisfied.

1. All records/transactions are logged into the system during the project implementation stage.
2. All records/transactions are preserved for a very long duration, i.e. even after project implementation is over.

The following points are important considerations to bear in mind:

1. User-friendly UI and integration with the World Bank and client systems

It is important to conduct a detailed analysis of the current environment and include the input from all entities (i.e. World Bank, PIUs, intermediaries, suppliers, etc.). This analysis should be the input to the design phase of the new system.

It is possible that the future production environment will create links to hundreds of external systems. Special attention should be given to the monitoring of the environment, e.g. detection and notification of failed links, submission of transactions occurred during downtime, etc.

2. Change management

Changes to operational procedures will be required to ensure that all parties involved in downstream transactions enter the required information in the new system, e.g. linking the trigger for disbursement to the existence of corresponding details in the new system. In the absence of rules mandating the data entry to the new system, it is unlikely that external parties will enter all the required information into the new system.

3. Handling of historical transactions (data migration)

It may not be possible to capture historical transactions in the new system for various reasons, including:

- A project may be closed;
- Technical difficulties in collection and submission of historical transactions; and
- No existing mandate to input the historical transactions into the new system.

As a result, the new system will only be adopted by newly launched projects.

4. Operating and owning blockchain nodes and off-chain data storage

It is important that any entity which runs the blockchain node or provides the support for off-chain data storage continues to provide the required support, even after a project is closed. As a result, it may not be possible to delegate this responsibility to entities which are only active during the project implementation phase. As most of the vendors have proposed, the actual documents will not be stored on the chain. The actual documents will therefore not be replicated on the various blockchain nodes. In this context, it is important that the entities hosting the off-chain databases provide the required guarantee that data are maintained properly for a considerable time in the future.

The following are general considerations related the production environment:

- Three environments will be needed for the new blockchain system, namely development, testing and production. Testing will be carried out in a parallel environment and could also involve test systems from the World Bank and other external entities.
- As multiple parties are involved, overall governance support is very important, i.e. everyone needs to be very clear about their respective roles and responsibilities.
- Due to the decentralized nature of the blockchain platform, any changes to the software should be jointly managed. All change requests should be tracked using a standard tool. Any change should only be moved to the production environment after the pre-agreed key controls are satisfied
- A robust software version control system should be used to provide complete view of changes and revisions.

3.4 Public vs Private Blockchain Model

Public Blockchain is a type of Blockchain which lets anyone read and write to the shared ledger. It also allows anyone to be part of this public Blockchain network in varying capacity and capabilities. But if anyone can be part of this public Blockchain network, who manages and owns it? While this topic is not addressed in this paper, the relevant question for this project is whether any future World Bank Blockchain enabled infrastructure should adopt the model of public Blockchain? Advances in blockchain technology have given us other models to consider, such as permissioned blockchain, which restricts access to partners/collaborators of the project, thus creating a blockchain business network. These collaborators are responsible for governing the blockchain. Permissioned blockchain differs from public blockchain in terms of functionality and security, and is typically adopted by enterprises, whose needs differ from public blockchains. Some of these functionalities are known and trusted participants and apply data confidentiality, system and business rules, security, scalability, formal governance and regulatory compliance. These needs guide enterprises towards a permissioned blockchain, where these needs can be met.

The disbursement traceability project team considered the following project requirements:

- The blockchain network should include World Bank client countries and partners, e.g. donors, NGOs, PIUs, etc.;
- Client country data should be confidential and available only to themselves and the World Bank;
- System and business rule guidelines have been defined and identified;
- Enterprise grade security is needed;
- The blockchain network should be scalable to provide transaction throughput in seconds, hence requiring a Proof-Of-Authority (POA) consensus model;
- To ensure regulatory compliance and governance over the solution, a consortium of World Bank, donors and client country would be needed.

3.5 Tokenization for Traceability

Applicability: The specific advantages inherent in the implementation of DLT include: (i) its distributed trust model; (ii) the resilient nature of technology solution; and (iii) the immutability of the information going on the Ledger. The implementation of DLT does not need or require a 'token' in its design. However, in the context of the business requirements and challenge statement, it is important to assess whether tokens would be an essential part of the overall DLT solution design, and how blockchain/DLT powered tokenization could provide capabilities to address the problem. Depending on how tokenization is used in the solution design, it could have different implications in the operationalization of the proposed technology solution. One of project team's objectives was to better understand some of the following open questions.

- Can the proposed DLT-enabled technology solution address the traceability and tracking of fund flows challenge, and ensure that the disbursement of funds meets its intended purpose at various levels of delivery chain without the use of tokens?

- What are the different tokenization models that could be applicable for the challenge under consideration?
- How can tokenization help in representing funds flow on blockchain with 'real value-transfer' taking place through traditional financial channels?
- What are the different operationalization models in the context of tokenization and related considerations that should be further assessed?

Key Learnings and Proposed Approaches:

- One of the proposed solution approaches is to realize the benefits of DLT for disbursement traceability without the use of tokenization. In this scenario, the platform would be used for primarily for the reporting of fund transfers, corresponding confirmations, and document notarization.
- Another potential approach is using proprietary digital tokens to represent the flow of funds on the blockchain. 'This approach could establish a more direct connection between real value transfer and the reporting that takes place on the DLT platform, thereby ensuring stronger disbursement traceability and confirmation that funds are being spent for their intended purpose. This approach will be beneficial if used in conjunction with DLT analytics capabilities for any reconciliation that would be needed between actual financial transfers and their tokenized representation on the DLT/blockchain platform.
- A third approach is the use of existing stable value tokens, which have incorporate mechanisms which provide a stable value digital representation of a fiat currency. Some commercial banks are also looking into issuing DLT-based stable value tokens and various other wholesale and retail payment technology innovations. This could help in enabling on-chain payments where new and emerging mechanisms for cash-in and cash-out could be explored.
- To gain acceptance and adoption for the proposed disbursement traceability technology platform, it may be important to consider not restricting the solution to only notarization purposes, but also for tokenization to enhance visibility and traceability. This could create added incentives for adoption.
- The team also explored and gained insights into various custodianship models and requirements that would need to be considered when utilizing tokenization capabilities. One of the key aspects of digital asset custody is how to securely and safely managing private keys. The custodianship capabilities of digital asset instruments therefore require additional diligence and excellent security.
- While utilizing tokenization, more emphasis is needed on KYC/AML, which may require new capabilities.

3.6 Forward Looking: Innovation Opportunities

Innovation in Payment Technologies: The growth of new emerging technologies, e.g. blockchain/DLT, AI and machine learning, mobile technologies, etc., have led to a growth in demand for new payment technologies. While focusing on the disbursement traceability challenge, the project team also examined emerging innovative payment technologies.

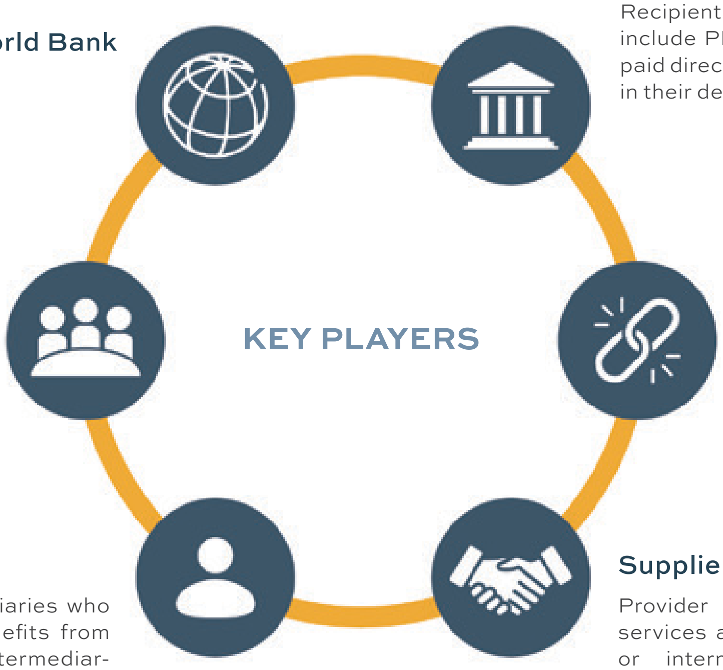
Many financial institutions are currently looking into leveraging the benefits of these technologies in making in wholesale and retail payment systems more efficient, these include: Interbank Innovation Network (IIN); institutional coins; so-called stable coins; CBDC; DLT-enabled payment platforms; and payment tech innovations. While various efforts are being directed towards payment technology innovation, the team recognizes that incorporating these new models poses different known and unknown risks which would require further assessment.

- *Use of existing so-called stable coin for disbursement:* There are stable coin platforms, public blockchain, which provide for so-called stable value currencies pegged to fiat currencies, and which can enable value transfer on-chain. This could help bring efficiency in value transfer in addition to tracking disbursement, especially further down the disbursement chain.
- *Use of cryptocurrencies for disbursement:* Can cryptocurrencies, such as Ethereum and Bitcoin, be leveraged for making disbursements? UNICEF has piloted the idea of using public cryptocurrencies, such as Ethereum and Bitcoin, to receive value transfer from donor organizations and use them to disburse/invest in pre-selected start-ups. This UNICEF project was launched to track the exchange of value and to better understand and equip the organization to a future-facing way of looking at digital finance. However, the use of cryptocurrencies would pose myriad risks and challenges in the context of the World Bank disbursement traceability challenge statements, including the volatile value of cryptocurrencies, data protection and privacy, regulation uncertainties, etc.
- Use of CBDCs (if and when they arrive): The team did not consider CBDC as part of this exploration; however, it is increasingly clear that various central banks are actively researching and exploring the idea of issuing natively digital currency backed by their country's central banks. Although, this is a more future-facing agenda and remains at the exploratory stage. This development could have implications for World Bank disbursements and enable digital currency initiatives.

The data privacy and confidentially requirements are addressed by permissioned Blockchain capabilities. However, considering the global scope of World Bank projects and the diversity of financial intermediaries, the different public blockchain platforms provide an opportunity to benefit from the innovation, accessibility, and immutability of these public ledgers.

DEFINITION OF PAYEES	
PIU/MoF Payee (Recipient)	Recipients of funds typically include PIUs or MoFs that get paid directly by the World Bank in their designated account.
Intermediary Payee	Additional layers of intermediary(ies) that receive payments from the PIU and either cascade payment down to other intermediaries or the ultimate citizen beneficiary.
Supplier Payee	Provider of goods and services as contracted by the PIU or intermediary in compliance with WB procurement policies and procedures.
Ultimate Citizen Payee	Ultimate citizen payee who may receive payments directly from the PIU or the intermediaries.

DEFINITION OF BENEFICIARY	
Ultimate Citizen Beneficiary	Ultimate citizen payee who may receive goods or services directly from the PIU, Intermediaries or Suppliers.



The World Bank

Borrowers (PIU/MoF)

Recipients of funds typically include PIUs or MoFs that get paid directly by the World Bank in their designated account.

Key Stakeholders

Stakeholders such as, Auditors, Participating Member Countries, Donors, Other MDBs.

Intermediaries
(NGOs, Agencies, Layers of government, etc.)

Additional layers of intermediary(ies) that receive payments from the PIU and either cascade payment down to other intermediaries or the ultimate citizen beneficiary.

Beneficiaries

Ultimate beneficiaries who may receive benefits from the PIU or the intermediaries or the suppliers.

Suppliers

Provider of works, goods, and services as contracted by the PIU or intermediary in compliance with WB procurement policies and procedures