

Overview

The *Bedrock Consortium* is a collection of international private sector companies that operate the *Bedrock Business Utility (BBU)*, an independent self-governed non-profit legal entity that serves as a public identity utility and operates as a self-sustainable directed fund project under [The Linux Foundation](#).



The BBU is intended to serve organizations that desire to participate in [digital trust ecosystems](#) and require an enterprise grade governance framework that will:

- Enforce permissioned-writes with contractual instruments that will conform to privacy regulations such as GDPR
- Maintain financial sustainability of the consortium members without the use of cryptographic tokens
- Establish a governing board so that no single organization owns the [Identity Utility Network](#)
- Require adherences to a specified open standards and protocols

To meet these requirements, the BBU operates as a *Linux Foundation Operational Project* (a Delaware series limited liability company) under its own governance framework. Consortium members pay annual membership fees and provide

supporting infrastructure to maintain a sustainable permissioned identity utility that is structured as an enterprise safe-space and purpose built for trusted commerce. The consortium leverages an independent [Utility Service Provider](#) as a fee-based administrator for the delivery of a [DID Ledger](#) associated with a unique DID Root Namespace, `did:bpu`.

This document serves as the *constitution* for the BBU and represents the official BBU Governance Framework (BBU-GF).

The governing body responsible for the BBU-GF is the *Governing Board*.

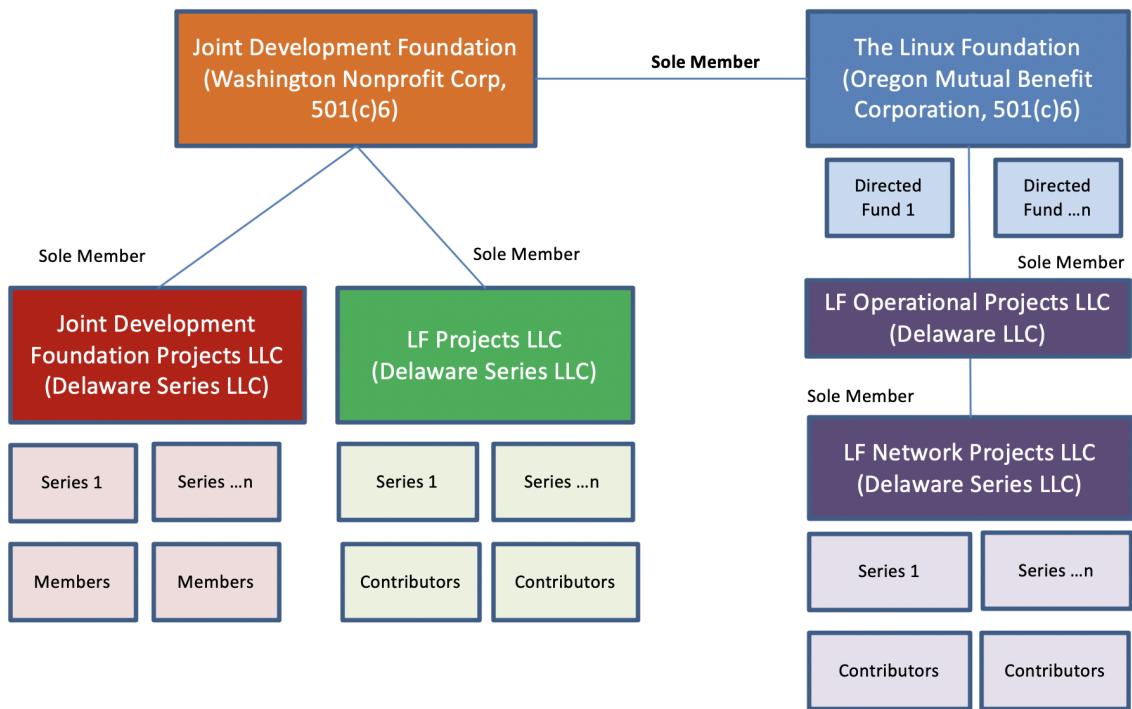
Consortium

Non-Profit Organization

The **Bedrock Consortium** ("Consortium") is an international non-profit association of members that share a common interest in collaborating on the delivery of the infrastructure and governance necessary for a dedicated and trusted public identity utility based on decentralized identity technology. The utility is intended to reliably serve the verifiability of both physical and online digital identity interactions. The Consortium is focused on the governance of a dedicated decentralized identity utility for the exchange of trusted data. The Consortium represents a formal Trust Community consisting of participating members that adhere to the *Bedrock Business Utility Governance Framework* ("BBU-GF").

Legal Entity Structure

The [Linux Foundation](#) (the "LF") is dedicated to building sustainable ecosystems around open source projects to accelerate technology development and industry adoption. It provides support for open source communities through financial and intellectual resources, infrastructure, services, events, and training. The LF also provides a proven legal structure for the establishment of open source projects as non-profit legal entities for members.



Entity	Purpose
The Linux Foundation, (Oregon Mutual Benefit Corporation, 501(c)6)	Legal membership entity for Directed Funds
LF Operational Projects LLC (Delaware LLC)	Legal entity for managing non-member use of a transactional entity.
LF Network Projects LLC, (Delaware Series LLC)	Holds trademark assets for series entities (open source technical projects).

Legal Entity Registration

The *Bedrock Business Utility Fund* (the “Directed Fund”), is a directed fund project of the LF. The Directed Fund serves two purposes:

1. Manage the operation and maintenance of the *Bedrock Business Utility* (“the Utility”), a LF Operational Project (a Delaware series limited liability company)
2. Support for the *Bedrock Consortium Project*, (the “Technical Project”), an open source project, a LF Network Projects.

Membership Signing Requirements

Participation in or use of a project entity may require the signing of one or more contractual instruments.

Entity	Signing Requirements			
The Linux Foundation (Oregon Mutual Benefit Corporation, 501(c)6)	Bedrock Business Utility Directed Fund	Sign LF Membership Agreement	Sign Participation Agreement	Sign Network Agreements
Members				
Non-Members				Sign Network Agreements (non-member)
LF Operational Projects LLC (Delaware LLC)				
LF Network Projects LLC (Delaware Series LLC)				
Bedrock Consortium Project Series LLC		Sign CLA (optional)		
Contributors				

Entity Type	Entity Name	Contractual Instruments
Directed Fund	Bedrock Business Utility Directed Fund	LF Membership Agreement, BBU Participation Agreement, and Utility Agreements.
Utility	Bedrock Business Utility	Utility Agreements
Technical Project	Bedrock Consortium Project	None

The BBU Participation Agreement binds members to project funding commitments, policies, etc. It also puts forth a project charter that addresses the governance of directed fund and customized requirements for *Utility Agreements*.

For details pertaining to *Utility Agreements*, see "Exhibit B" of the Bedrock Business Utility Fund Charter as articulated in the [BBU Partnership Agreement](#).

The *Bedrock Consortium Project* does not require the signing of a *Contributors License Agreement (CLA)*.

Consortium Name

Participants in the Directed Fund are members of the Bedrock Consortium. Our membership shares a keen interest towards the establishment of trusted commerce. They believe in a set of fundamental privacy by design principles while mitigating financial and regulatory compliance risks.

The term "Bedrock" carries two pertinent meanings:

1. Gold accumulates at this solid foundational layer of the earth because water can't "wash it down" any further. The implication here is that our public identity utility ledger is the bedrock for business trust worldwide.
2. A "bedrock" principle is one that forms the basis for others principles. Our public identity utility ledger aims to provide the foundational principles for the exchange of trusted personal data.

Governing Board

The Consortium will appoint a Governing Board as the governing body of the Directed Fund. The Governing Board will be comprised of representatives from membership as outlined in "Exhibit B" of the Bedrock Business Utility Fund Charter. See [BBU Partnership Agreement](#).

Bylaws

The Governing Board is responsible for establishing and maintaining the governance framework for the operation and administration of the *Bedrock Business Utility* ("BBU") along with the bylaws for the Consortium. See [BBU Partnership Agreement](#).

Motivation

Global Growth

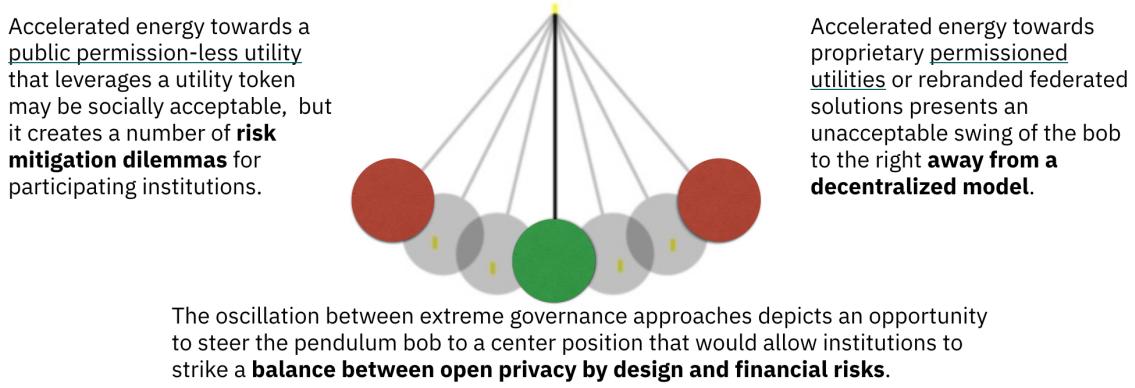
The [Sovrin Foundation](#) entered into the decentralized identity market as a permissioned public ledger. Over several years, it evolved into an industry brand associated with decentralized identity. It represents more than an instance of a decentralized identity network based on a DLT, it is a trusted community of like-minded people and institutions from a variety of geographic regions and industry sectors. The Sovrin Community aspires to help all the entities (citizens, governments, businesses, devices) of the world to fix identity for both online and physical interactions.

During this same period, a global spotlight on privacy protection has spawned regulation such as GDPR and CCPA, which complements the spirit of the decentralized identity movement. However, these regulations also place additional financial risk and compliance constraints on businesses that desire to participate in and contribute to this privacy protection movement.

At the same time, the grassroots energy focused on “identity for all” shifted or accelerated the thinking within the Sovrin Community towards a public permission-less utility that leverages a cryptographic utility token. These philosophical changes, while socially acceptable, create a number of risk mitigation dilemmas for participating institutions. As a result, some businesses have exited the community while others have been hesitant to join.

Meanwhile, the hype around decentralized identity also spawned new federated identity systems like the [Global Association for Digital Identity \(GADI\)](#) from the [DID Alliance](#) that promote marketing messages under the banner of decentralized identity while actually establishing architectures that contradict the core [Privacy by Design Principles](#). GADI architecture enables a collection of Digital Address Providers (DAPs) to centrally manage identities for individuals whereas the Sovrin Community advocates for an architecture that allows identities to be managed without reliance on any external administrative authority.

The Sovrin Community is comprised of minimally two disparate market segments. Both segments can agree on an Open by Design governance approach. While the members within each market segment may require incompatible governance models, both segments adamantly disagree with any deviation from an open approach at the technology or governance levels.



To counter the pendulum bob swinging so far to the left, we have witnessed proposals for alternative proprietary solutions that reflect an unacceptable swing of the bob to the right. This oscillation between extremes depicts an opportunity to steer the pendulum bob to a center position that would allow institutions to strike a balance between open privacy by design and financial risks.

Reality Check

In the Autumn of 2019, early prospective members of the Bedrock Consortium responded to this quest to bring the pendulum bob back to center. The result was the formation of the Bedrock Business Utility which was intended to address three key concerns:

1. Policy Gridlock
2. Permissioned Safe Zone
3. Token-free Economics

Policy Gridlock

The Sovrin approach for decentralized identity was to tackle it at global scale. The Sovrin Community, much like the global societies it sought to represent, struggled with the formation of policies that can be embraced all at once by its members. The balancing of diversity goals at the operational level, risk mitigation for privacy regulation compliance, identity access for all, and the sustainability of a stable and reliable network was a non-trivial exercise. The technology adoption lifecycle teaches us that we cannot assume that all interested stakeholders will be able to embrace and adopt the technology at the same rate.

The Sovrin Foundation needed to find ways for it to [a] stay true to its vision; [b] aid all stakeholders on their decentralized identity journey; and [c] remain financially sustainable. ↩

Businesses and Governments around the world must be able to balance risk mitigation and technology adoption if Sovrin was to be an open community for all. Additionally, all stakeholders must accept the fact that a single network (DID ledger) cannot serve the entire globe. As an example, the Sovrin Network was based on Hyperledger Indy, which like many consensus algorithms, carries an expected threshold of optimal validator nodes, thereby limiting the scalability of a single network.

The decentralized identity community cannot afford to have disputes at the network level. We must focus on market creation not market bifurcation. We live in a heterogeneous world of networks where interoperability is paramount. ↩ A single network cannot meet the needs of everyone and continued attempts to do so will minimally yield increased complexity and confusion. These facts became reality within the Sovrin Foundation as it became difficult to obtain closure after nearly a year on Version 2 of the Sovrin Governance Framework.

The Sovrin Foundation was in gridlock throughout all of 2019 due to apprehension between policy decisions that were necessary for one market segment and uncomfortable for another. These concerns impacted the business market segment as well as external coalitions such as FINDY and KIVA who may have desired to have their own governance framework while participating in the Sovrin Community. One approach to breaking the gridlock while still enabling two market segments to co-exist was to establish a community bound to a common

vision but comprised of safe-spaces for each segment to establish their own governance.

Permissioned Safe Zone

Preventive measures for avoiding the possible insertion of personal data into an immutable ledger has been the focus of much discussion. While many have agreed that a 100% guarantee is not possible, the implementation of a public write model only increases such exposure thereby making interested stakeholders more apprehensive to embrace a permission-less governance model. A diligent effort was made within the Sovrin Foundation to address the regulatory risks (i.e.: CCPA, GDPR) associated community stakeholders. In collaboration with legal experts, the community established a series of contractual instruments that addressed these risks for each stakeholder under both the public-write and permissioned write models. Unfortunately, this effort resulted in a greater degree of complexity to the governance framework. It also yielded an increase in costs for Stewards that need to comply with a broader set of technical and operational requirements.

One approach to reducing the complexity of governance policies was to transition the existing Sovrin Network (DID Ledger) into a dedicated ledger for public write access and then add a new DID Ledger that would operate under a separate governance model for permissioned writes.

Token-free Economics

The Sovrin Foundation spent a huge amount of money investing in a new Governance Framework that favors the use of a crypto-token to enable a payment model for public-write interactions with a DID Ledger. The combination of public write access coupled with the conveniences of a payment token would open identity access up to a very diverse community that is currently unable to establish a trusted identity reputation.

While the social benefits of such an approach are appealing to many, the ability for many enterprises and some governments to embrace the use of crypto-tokens in the first half of 2020 was limiting. The community needed to explore a compromise which allowed two market segments to coexist. We needed to

establish a community bound to a common vision but comprised of safe-spaces for each segment to establish their own governance.

Common Ground

The pathway to a common vision for decentralized identity has always been rooted in open standards and open source communities. As a community, we agree on:

- an Open by Design approach based on open standards
- avoidance of with any deviation from an open approach at the technology or governance levels
- the need to support a network of networks model that enables disparate market segments to deploy different governance

Fundamentally, no single organization can own a network (system of ledgers) and the network must be built upon open standards and protocols where interoperability has been achieved.

Transition

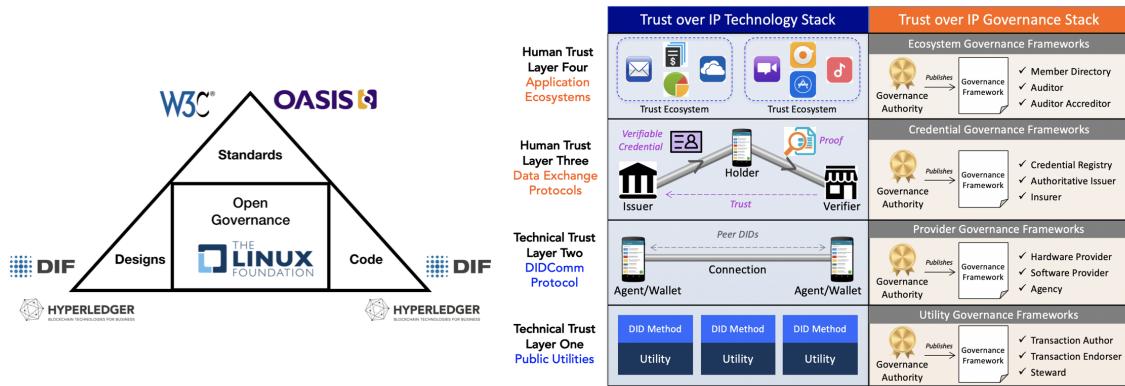
In March 2020, the Sovrin Foundation's ongoing attempts to serve multiple disparate market segments under a single governance framework came to an abrupt halt when financial constraints finally triggered the need for a change.

The [ToIP Foundation](#) offered all community stakeholders the flexibility to establish one or more Identity Utility Networks that can serve the needs of the diverse segments of the Sovrin Community and beyond.

Digital Trust Marketplace

As the proliferation of decentralized identity utility networks continued to increase, the global identity industry needed a way to categorize and position independent networks for discovery, access and trust. The [Trust over IP \(ToIP\) Foundation](#) addressed this growing need by establishing a collaborative

community that frames the technology and governance infrastructure necessary to support an *interoperable digital trust marketplace*.



In collaboration with [ToIP Utility Foundry Working Group](#), organizations can establish independent self-governed and self-sustainable public utilities, at layer one of ToIP Architecture. This architecture establishes human trust between peers—trust between real-world individuals and organizations and the things with which they interact (devices, sensors, appliances, vehicles, buildings, cities, etc.). The ToIP Architecture is technology agnostic, allowing solutions to be constructed using open building blocks (standards, specs and code) and provides a complete architecture for Internet-scale transitive trust that integrates cryptographic verifiability at the technical machine layer with human trust at the business, social, and legal layers.

Membership

The concepts outlined herein provide an informational synopsis for the operation of the Bedrock Business Utility and participation in the Bedrock Business Directed Fund Project. The executable [BBU Participation Agreement](#) (the "Participation Agreement"), specifically [Exhibit B](#) and [Exhibit C](#), supersedes this content.

Utility Infrastructure Requirements

The Utility is an instance of a [ToIP Layer One Public Utility](#) based on [Hyperledger Indy](#) ("Indy"). In order to establish an operational budget for the Utility, several infrastructure assumptions must be considered.

1. Budgetary requirements dictate how much revenue is required to keep the Utility sustainable.
2. Distributed ledger technologies, like Indy, leverage consensus algorithms that come with an optimal consensus threshold. This threshold value dictates the number of validator nodes required to operate the Utility. To meet the needs of a decentralized ledger, each validator node must be operated by an independent and unique participant. Therefore, a quantity requirement associated with one or more classes of members will be tied to the number of required validator nodes. Validator nodes may also be referred to as *utility infrastructure nodes* or *Stewards* from a historical [Sovrin Foundation](#) context.

A balance between budget requirements and technology limitations will define the number of validator nodes required to operate the Utility. Initially this will be set at twenty-five (25) utility infrastructure nodes. The set of active nodes on the network will be periodically pulled from a pool of available nodes.

Validator Node Pool

In order to efficiently operate the ledger associated with the Utility, a combination of production, test, and development environments are necessary. The Governing Board is responsible for defining the requirements associated with the validator

pool. It is important to note that such Governing Board decisions will be influenced by both technical performance restrictions as well as budgetary demands.

Framework Facet	Required Quantity	Comment
Governing Board Seats	7	Minimum Governing Members. Governing Board seats can increase but MUST not exceed 15
Minimum Production Pool Size	19	Considers production and Governing Board factors.
Minimum Test Pool Size	3	Ledger used by Utility Service Provider and Technical Project contributors.
Minimum Development Pool Size	3	Ledger used by Utility Service Provider and Technical Project contributors.
Minimum Total Pool Size	25	Considers requirements across all environments.

Steward Population Dynamics

The number of Board of Director seats SHOULD be consistent as the population of Stewards (Governing and Operational Members) increases.

Board of Director Seats	Required Stewards	BoD%	
7	25	0.28	
9	36	0.25	
11	44	0.25	
13	52	0.25	
15	60	0.25	

The Governing Board MUST maintain a **FIFO Waiting List** of Operational Members that have maintained consistent membership. This list shall be used to offer new Governing Board seats upon availability due to attrition or growth.

Membership Types

Building on our [Glossary](#), participants in the Consortium are referred to as *Trust Community Members*. These business entities agreed to participate in the *Trust Community* known as the Bedrock Consortium. Participation in the Consortium is possible via formal legal contracts or membership agreements.

Annual Membership

Private sector entities (businesses) can join and renew membership on an annual basis under three possible membership types:

Membership Type	Validator Node Hosting Required	Governing Body Participation Required	Authorized Endorser Privileges (Ledger Writes)
Governing Member	Yes	Yes - 1 Per Governing Body	Yes - Unlimited
Operational Member	Yes	Yes - 2	Yes - Unlimited
Subscriber	No	No	Yes - Limited

1. Governing Member:

- **Description:** Members that are willing to contribute to the infrastructure, management, and financial needs of the Utility. Minimally, this requires the member to contribute a *Validator Node* to the operation of the Ledger.

- **Ledger Roles:**

- a. *Validator Node:* Must host one or more utility infrastructure nodes as defined in [Exhibit C](#) of the Participation Agreement.
- b. *Transaction Endorser:* APPROVED for the endorsement for *Transaction Author* write requests.

- **Restrictions:**

- a. Membership is limited to the number of Board of Director seats available.
- b. A FIFO waiting list is maintained by Governing Board to allow for new members to fill voids left by exiting members.
- c. Must sign the required [Utility Agreements](#) as set forth in the Participation Agreement.
- d. Utility Service Providers MAY NOT be a Governing Member.
- e. Utility Service Providers MAY NOT participate in the Finance Committee.

- **Benefits:**

- a. A single representative on the Board of Directors.
- b. Appointment of representatives to any Committee within the Directed Fund.
- c. Approval, pending signed Utility Agreements , to act as a Transaction Endorser.
- d. Write Transactions as a Transaction Endorser as defined in Exhibit C of the Participation Agreement.

2. Operational Member

- **Description:** Members that are willing to contribute to the infrastructure, management, and financial needs of the Network. Minimally, this requires the member to contribute a *Validator Node* to the operation of the Ledger.

- **Ledger Roles:**

- a. *Validator Node*: Must host one or more utility infrastructure nodes as defined in Exhibit C of the Participation Agreement.
- b. *Transaction Endorser*: APPROVED for the endorsement for *Transaction Author* write requests.

- **Restrictions:**

- a. Must sign the required Utility Agreements as set forth in the Participation Agreement.
- b. Membership is limited to the number of nodes required to maintain optimal consensus performance. The optimal limit here must take into consideration a balance with decentralization requirements. The Governing Board will annually determine the number of nodes required to meet both consensus, decentralization, and budgetary requirements.

- **Benefits:**

- a. Appointment of representatives to any Committee within the Directed Fund.

- b. Approval, pending signed Utility Agreements , to act as a Transaction Endorser.
- c. Write Transactions as a Transaction Endorser as defined in Exhibit C of the Participation Agreement.
- d. Members with continuous participation, can reserve a position to be invited as a Governing Steward via a FIFO waiting list.

3. Subscriber

- **Description:** Members that are willing to be responsible for the endorsement of transactions to the ledger.
- **Ledger Roles:**
 - a. *Transaction Endorser*: APPROVED for the endorsement for *Transaction Author* write requests.
- **Restrictions:**
 - a. Must sign the required Utility Agreements as set forth in the Participation Agreement.
- **Benefits:**
 - a. Appointment of representatives to any Committee within the Directed Fund.
 - b. Approval, pending signed Utility Agreements , to act as a Transaction Endorser.
 - c. Write Transactions as a Transaction Endorser as defined in Exhibit C of the Participation Agreement.

Non-Membership Roles

1. Transaction Author

- **Description:** Any entity (member or non-member) that is the submitter of a write transaction. **Ledger Roles:**
 - a. *Transaction Author*: Interacts with a *Transaction Endorser* for the processing of write requests.

- **Restrictions:**

- a. Only the transaction types outlined in the Utilities [ledger access policies](#) and [ledger data policies](#) are permitted.
- b. MUST sign the [Utility Agreements](#) as defined in the Participation Agreement.

- **Benefits:**

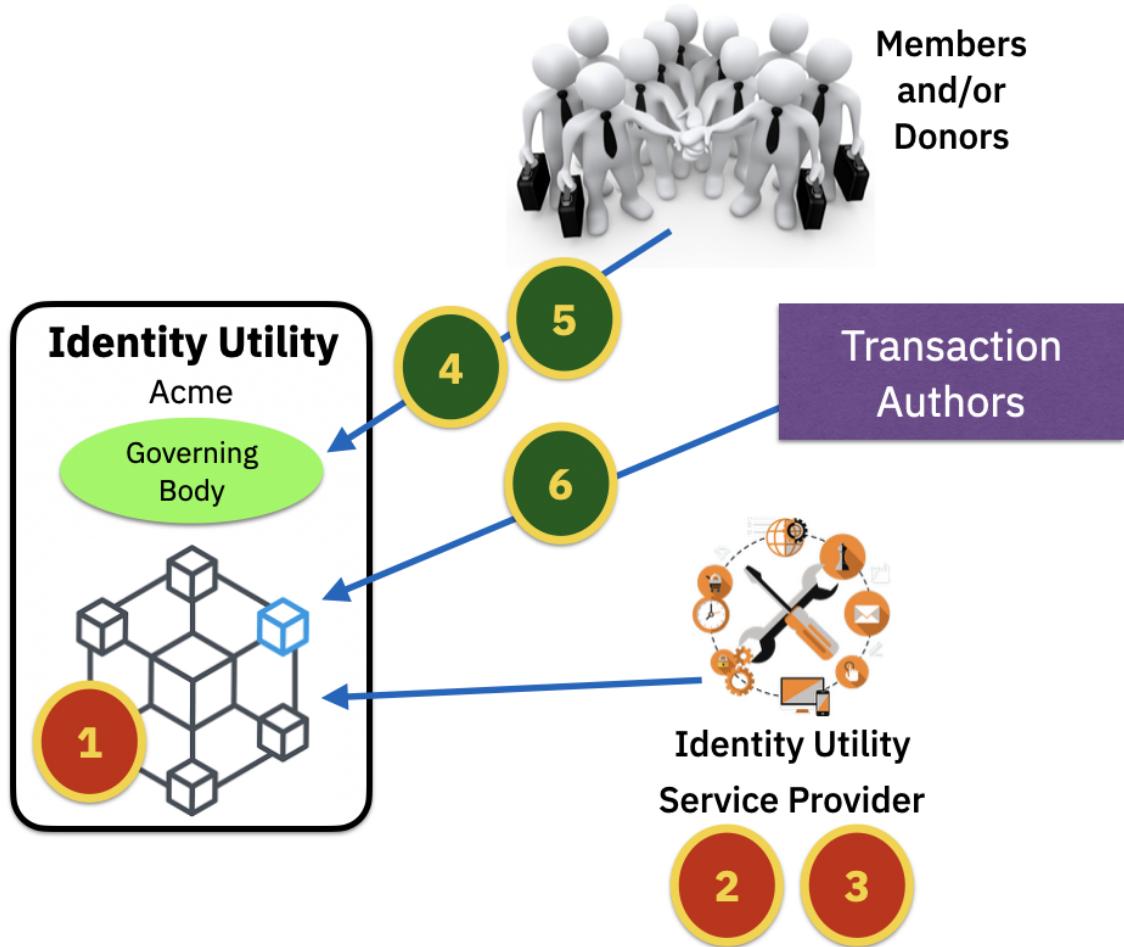
- a. Ability to use ledger for decentralized identity interactions.

2. Contributors to the Technical Project

- **Description:** A category of membership that is limited to Associate Members of the Linux Foundation. This membership category is limited to participation in Committees within the Technical Project.

Business Model

When a consortium of organizations such as those associated with the Bedrock Business Utility come together to operate a public identity utility there are several factors that need to be considered with respect to a sustainable business model.



Identity Utility Networks have specific income and expense characteristics that are addressed by the principles, policies and procedures outlined in their governance frameworks.

Expenses	Income	
1. Node Hosting	4. Consortium Membership	
2. Network Operation and Maintenance Services	5. Community Donations	
3. Consortium Governance	6. Transaction Revenue	

Utility Operations

Node Hosting

General Concept

The deployment of decentralized identity solution based on distributed ledger technology (i.e.: blockchain ledgers) implies that there will not be a single centralized entity that owns and operates the ledger or the nodes attached to the ledger. The governing body of a distributed ledger owns the responsibility for defining the technology that is used to establish and run the ledger. However, it is the responsibility of each node owner to provide an operational compute node that meets the requirements of the governing body. Fulfillment of the node owner's responsibilities comes at a cost regardless of their decision to manage the node themselves or to pay a hosting provider.

Some governing bodies may place diversity requirements on node owners. These requirements may include restrictions such as but not limited to:

- Number of nodes hosted in a specific data center
- Number of nodes hosted in a geolocation
- Number of nodes running on the [IaaS](#)
- Number of nodes hosted by the same hosting provider

BBU Perspective

Any member of the Bedrock Business Utility that is [required to host a utility infrastructure node](#) is considered a Steward and is responsible for the financial

demands of hosting a node. Such expenditures are considered out-of-pocket expenses and are not related to the members annual membership obligations. However, the BBU-GF does recognize the infrastructure contributions of Stewards and MUST adjust membership fees accordingly.

Stewards MUST adhere to the [Member Technical and Organizational Policies](#) set forth in the Controlled Documents of the BBU-GF.

Network Operation and Maintenance Services

General Concept

The management of a distributed ledger MUST be administered by skilled personnel that is familiar with:

- designing, building, testing and deployment of networks based on [distributed ledger technology](#) (DLT)
- maintaining and releasing reliable versions of a DLT
- onboarding and configuration of nodes
- monitoring and tuning of Hyperledger Indy networks

The governing body of a public identity utility is responsible for hiring in-house or external resources to accomplish these tasks. The cumulative costs of such services have a direct impact on the financial budget for the Utility.

The [ToIP Foundation](#) recognizes the importance of the services of Utility Service Providers and has established a dedicated *Utility Foundry Working Group* to aid governing bodies in selection and hiring of such providers. For example, access to proven *request-for-proposal* (RFP) templates. Typically, a governing body would initiate a bidding process for an annual contract with the necessary service-level-agreements (SLAs).

BBU Perspective

The Governing Board of the Bedrock Business Utility with advice from the *Finance Committee* and *Technical Steering Committee* will hire personnel responsible for the operation and maintenance of the Utility.

Consortium Governance

General Concept

The development and maintenance of a governance framework complete with legal instruments is no small task. The governing body of a public identity utility may establish a *Governance Framework Working Group* to handle the effort internally or the governing body may leverage the services of a Utility Service Provider for all or portions of the effort.

The [ToIP Foundation](#) recognizes the complexity of this task and has established a dedicated *Utility Foundry Working Group* to provide templates for governance frameworks along with access to experienced service providers.

BBU Perspective

The Governing Board of the Bedrock Business Utility leverages the inexpensive volunteer services of its members to form a *Governance Framework Working Group* that is responsible for the task.

Utility Revenue

Consortium Membership

General Concept

A public identity utility serves the needs of interested stakeholders by allowing for both read and write transactions. While read transactions are generally publicly accessible and free, write transactions are typically fee-based. Governing bodies can treat write transactions as an entitlement of membership and charge members for participation in the Utility.

BBU Perspective

The Governing Board of the Bedrock Business Utility publishes a [fee schedule](#) for participation in the Utility. These fees are the only guaranteed source of income.

Community Donations

General Concept

Meeting budgetary requirements via subsidized donations is not a recommended business model. However, donations are always possible and often welcomed.

BBU Perspective

While the Governing Board of the Bedrock Business Utility MAY accept donations, such income is not an assumed source of income.

Transaction Revenue

General Concept

Users of a permissioned ledger, known as Transaction Authors, have a desire to submit transactions to the Utility but they may not own the entitlements to perform those writes. The governing body of a public identity utility may charge fees for write access. They may also charge different fees for the different types of data writes allowed to the ledger. Transactional revenue can be accomplished in a number of ways such as but not limited to:

- Centralized endorser operated by the Utility
- Utility tax on endorsers who collect directly from Transaction Authors
- Selling write entitlements to endorsers and/or Transaction Authors

BBU Perspective

The Bedrock Business Utility Governance Framework **does not** collect revenue from transaction fees. The exchange of payment (value) between the Transaction Endorser and a Transaction Author is *out-of-scope*. Transaction Endorsers are free to charge any fee they desire for access to their write transaction entitlements.

Pricing

Disclaimer

The concepts outlined herein provide an informational synopsis for the use of the Utility and participation in the Directed Fund. The executable [BBU Participation Agreement](#) (the "Participation Agreement"), specifically [Exhibit C](#), supersedes this content.

Currency

Unless specified otherwise, all fees are in USA Dollars.

Membership Rates

The membership levels and associated fees are listed below.

Membership Class	Annual Membership Fees	Node Hosting Requirement	Write Transaction Entitlements
Governing Member	TBD	1	Unlimited
Operational Member	TBD	1	Unlimited
Subscriber	TBD	0	50

Subscription Packages

Subscriber membership comes with a preset level of transaction entitlements per annual membership. Additional transactions can be acquired per annum according to the following table. While a Subscriber may purchase an unlimited

number of entitlement packages, all unused transactions expire at years end without rollover./

Transaction Entitlements	Package Cost
50	TBD

Process

Membership

Members, excluding Associates, must be members of the [Linux Foundation](#) to qualify as a member of the BBU. Refer to the legal and fee requirements outlined in the Participation Agreement. For instructions on how to becomes a member, please refer to [getting started](#).

Note: See [Issue 10](#) regarding Join v. Contact Us.

Subscription Plans

Please visit the [BBU Subscription Procurement](#) website.

Usage

Non-members who desire to submit transactions to the Utility will need to contract directly with members who are providing Transaction Endorser services. The BBU has no authority over the fee schedules associated with the services of Transaction Endorsers. Each Transaction Endorser can use and / or sell their transaction entitlements as they deem appropriate.

Master Document

Preface

This is an official document of the Bedrock Business Utility Governance Framework ("BBU-GF"). If you have comments or suggestions, we invite you to submit them using our [issue tracker](#). If you are interested in joining the Bedrock Consortium, please feel free to [contact us](#).

Version Control

- **Version:** 0.2
- **Governing Board Approval Date:** TBD
- **Comments:** Ratification of the BBU-GF will take place upon the formation of the Governing Board (at first meeting).
- **Status:** BBU Governance Framework Working Group is currently developing the BBU-GF.

Acknowledgements

This document was produced on behalf of the BBU Governing Board by the BBU Governance Framework Working Group.

Introduction

The purpose of the Bedrock Business Utility is to provide a decentralized global public utility for trusted commerce. The Bedrock Governance Framework (the "BBU-GF") serves as the *constitution* for the *Bedrock Business Utility*. It represents an instance of a [ToIP Layer One Public Utility Governance Framework](#) under the guidance of the [ToIP Utility Foundry Working Group](#).

toip-stack

The BBU-GF leverages the principles, policies, terminology, and standards necessary to enable trusted digital commerce based on decentralized identity.

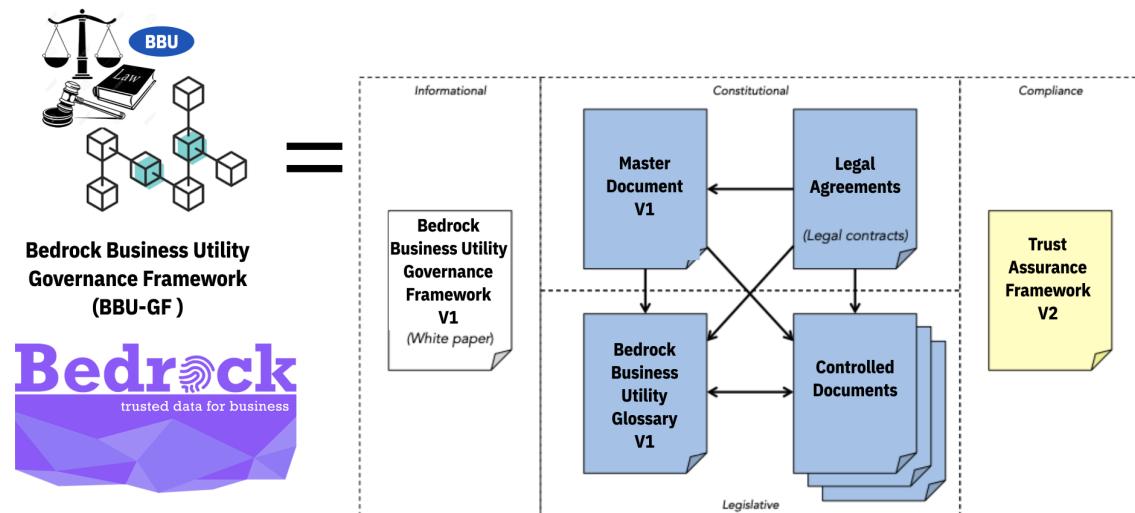
A key objective of the BBU-GF is to address any concerns or risks that Consortium members may have as Utility participants. For example, compliance with Data Protection Regulations such as the EU General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA).

The purpose of the Bedrock Consortium is to administer decentralized governance for Bedrock Business Utility.

Governance Framework

Governance Documents

The BBU-GF formally consists of a set of interrelated documents that collectively form the governance model for the Directed Fund and the Utility that the Consortium manages. The documents are organized in three (3) categories; Blue = Normative, Yellow = Assessment, White = Informative.



Category	Name	Description
Primary (White)	Bedrock GF Whitepaper	Introduction to the Bedrock Governance Framework Version 1
Primary (Blue)	Bedrock Governance Framework (BBU-GF) Master Document	The “constitution” of the Consortium, this document defines the purpose, core principles, and core policies, and also references all other documents in the GF.
Primary (Blue)	Bedrock Glossary	A comprehensive glossary of terms used throughout all the BBU-GF documents
Primary (Yellow)	Bedrock Trust Assurance Framework	This document defines criteria and processes for assessing conformance of consortium stakeholders to the policies of the BBU-GF.
Legal (Blue)	Bedrock Business Utility Participation Agreement	Contractual instrument between the Consortium and a member.
Legal (Blue)	Bedrock Steward Agreement	Contractual instrument between the Consortium and a Governing or Operational Member.
Legal (Blue)	Bedrock Steward Data Processing Agreement	Contractual instrument between the Consortium and a Governing or Operational Member.
Legal (Blue)	Bedrock Transaction Endorser Agreement	Contractual instrument between the Consortium and a Governing, Operational or Subscriber Member.
Legal (Blue)	Bedrock Transaction Endorser Data Processing Agreement	Contractual instrument between the Consortium and a Governing, Operational or Subscriber Member.
Legal (Blue)	Transaction Author Agreement	Contractual instrument between the Consortium and any person or organization initiating a write transaction to the Utility.

Core Principles

See [BBU Principles](#).

Core Policies

In keeping with all Core Principles and especially the Decentralization by Design and Security by Design principles:

1. Policies, practices, procedures, and algorithms governing participation of [Stewards](#) and operation of Nodes MUST follow all Core Principles.
2. The Consortium MUST publish the following Controlled Documents managed as specified by BBU Governing Bodies: a. Member Business Policies b. Member Technical Policies c. Ledger Access Policies

Inclusion

In keeping with the Inclusive by Design principles but in recognition of the permissioned write structure of the Bedrock Business Utility:

1. Read access to the Bedrock Business Utility MUST be open to all types of entities.
2. Write access will be limited to members and non-members in good standing within the Consortium.
3. Write access will be limited to members and non-members that have signed the necessary [Utility Agreements](#). See [Exhibit B](#) of the Participation Agreement.

Trust Assurance

In keeping with all Core Principles and especially the Decentralization by Design principles:

1. The Consortium MUST specify policies, practices, and procedures for assessing conformance to the Bedrock Governance Framework by

publishing and maintaining the Bedrock Trust Assurance Framework as a Controlled Document managed as specified by BBU Governing Bodies. The Controlled Documents may leverage resources and guidance from the TolP Foundation.

2. The Bedrock Consortium MUST publish a Bedrock Trust Mark Policies as a Controlled Document managed as specified by BBU Governing Bodies.

Economics

In keeping with the Sustainability principle:

1. The Consortium MUST publish the Bedrock Economic Policies as a Controlled Document managed as specified by BBU Governing Bodies in conjunction with Consortium legal counsel.
2. The Consortium MUST manage Ledger Fees and any mechanism used for paying them to ensure economic viability and sustainability for the Consortium to keep with its charter as a non-profit public trust organization.
3. The Consortium MAY retain a qualified Auditor to publish an annual public audit of Consortium finances.

Governance

The Bedrock Governance Framework Master Document and the Controlled Documents listed in Appendix A shall be revised from time to time. The policies in this section govern this process and procedures for managing document lifecycles.

General

1. The Consortium MUST publish BBU Governance Bodies as a Controlled Document managed by the Board of Directors.
2. BBU Governance Bodies MUST specify the Sovrin Governing Body for each Controlled Document.

3. All BBU-GF documents, including Controlled Documents, MUST use keywords in policies as defined in [IETF RFC 2119](#).
4. All BBU-GF documents MAY be revised to add non-normative content, such as references to appendices, white papers, or other explanatory materials, without triggering a formal revision review process as defined in this Governance Section .

Source Control

All BBU-GF documents will reside in a [Github source control repository](#) and will use the associated [Issue Tracker](#) for change management.

Approved Framework Process

1. Stable versions of the BBU-GF must be approved by the Board of Directors.
2. Approved versions need to be specified in the `Version Control` section of this document.
3. A static PDF file associated with the approved version MUST be stored in the `/pdf/approved` folder of the GitHub repo.
4. [Appendix A](#) of this document must be updated to point to the newly approved PDF file.

Master Document Revisions

These policies apply to any normative revision to the present document, exclusive of [Appendix A](#). 1. Revisions to the BBU-GF Master Document MUST respect the Purpose and Core Principles. 2. The commencement of any revision process MUST be publicly announced by the Consortium no later than the time of commencement. 3. Decisions in the revision process is restricted to the Governing Board and SHOULD consider input from all BBU members. 4. Proposed revisions MUST be publicly announced by the Consortium. 5. Revisions MUST be approved by a supermajority vote of at least two-thirds of the Governing Board and before the revision takes effect.

Controlled Document Revisions

These policies apply to any normative revision to the Controlled Documents listed in Appendix A . 1. The list of Controlled Documents in Appendix A, as well as each Controlled Document on that list, MAY be revised independently from the BBU-GF Master Document (the present document). 2. A Controlled Document MUST be stored in and use the source control mechanisms established in this Governance Section . 4. Revisions to a Controlled Document MUST be approved by the Governing Board before the revision takes effect.

Appendix A: Controlled Documents

The following Controlled Documents are normative components of the BBU-GF. All framework content is published by the Consortium in three forms:

1. A static PDF document representing the entire governance framework in a single document.
 - [Latest compilation of material from the GitHub Repo](#)
 - [Official Governing Board Approved Version](#)
2. A sub-section of the [BBU website](#) so that all documentation is easily navigated.
3. Independent markdown files (`.md`) in the [GitHub Repo](#).

Definitions

Document Name	Description	Governed By
BBU Glossary	Definitions of all terms used in the BGF	Governance Framework Working Group
Governing Bodies	Definitions of governing bodies within the Consortium	Bedrock Governing Board
Ledger Transaction Data	Defines the data and metadata process by a Steward Node	Technical Steering Committee

Specifications

Document Name	Description	Governed By
Decentralized Identifiers	Specification for DIDs and DID documents	W3C Credentials Community Group
BBU DID Method 1.0 Specification	Specification for the BBU DID Root Namespace. See Issue 13	Technical Steering Committee
Verifiable Credentials Data Model 1.0	Specification for verifiable credentials	W3C Verifiable Claims Working Group

Policies

Document Name	Description	Governed By
Governing Body Policies	Chartering and functioning of BBU Governing Bodies	Governing Board
Ledger Access Policies	Read and write access to the Bedrock Business Utility	Governance Framework Working Group
Member Business Policies	Member qualification, enrollment, and operational status	Membership Committee
Membership Technical Policies	Technical requirements for operating and protecting components of the BBU infrastructure.	Technical Steering Committee
Economic Policies	Budgetary policies for the BBU.	Finance Committee
Trust Mark Policies	Acceptable uses of the Bedrock Trust Mark	Governance Framework Working Group

Frameworks

Document Name	Description	Governed By
Trust Assurance Framework	Trust assurance for BGF actors	Governance Framework Working Group

Glossary

The Industry working on a convergence of industry terms between several glossary efforts, namely:

- [ToIP Glossary](#)
- DIF Glossary Working Group](<https://dif.groups.io/g/glossary>)
- [Sovrin Glossary](#)
- [NIST Glossary: A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems \(p50-51\)](#)

The contents herein are considered additional terms specific to the **Bedrock Business Utility**.

Note: See [BBU Issue 12](#)

Steward

A general term for an organization that is responsible for providing and maintaining a portion of the infrastructure necessary to establish a public identity utility. Minimally, the organization must meet the requirements to be a member of the public identity utility and must operate at least one `Node`.

Node

A computer network server running an instance of the code necessary to operate a distributed ledger or blockchain. In the Bedrock Consortium, a Node is operated by a Steward running an instance of the Bedrock Open Source Code to maintain the Bedrock Business Utility (or DID Ledger). A Node must be either a Validator Node or an Observer Node.

Bedrock Open Source Code

The computer software that is installed on all Nodes associated with the Bedrock Business Utility (BBU). This code determined by the Bedrock Board of Directors. The BBU adheres to code selection and version guidance provided by the Technical Steering Committee ("TSC") of the Bedrock Consortium Project. The TSC collaborates within the Hyperledger Indy Project of the Linux Foundation to establish a TSC approved version of Hyperledger Indy within the the Bedrock Code Repository managed by the TSC.

Bedrock Ledger Environments

The corpus of DID Ledgers used by the Bedrock Consortium to operate the Bedrock Business Utility. For example: `prod`, `test`, and `dev`.

DID Namespace

Building on URI Standards, the DID Specification allows for both root namespace (`did:xxx`) and sub-namespace (`did:xxx:yyy`) conventions.

Governing Body

An organization or consortium that is responsible for the management of an Identity Utility Network.

Backbone Network

A distinct system of domain specific ledgers operated by decentralized peer nodes and associated with a DID Namespace. Governed by its own governance framework. See also *Identity Utility Network*.

Peer-Net (*Deprecated*)

A distinct system of domain specific ledgers operated by decentralized peer nodes and associated with a DID Namespace. Governed by its own governance framework. See also *Backbone Network*.

Network of Networks

A decentralized collection of discoverable and interoperable Identity Utility Networks. The internet is an exemplar of a network of networks structure based on DNS and URI standards.

DID Ledger

A distinct system of domain specific ledgers operated by decentralized peer nodes and associated with a DID Namespace. See *Identity Utility Network (IUN)*

Identity Utility Network (IUN)

A distinct system of domain specific ledgers operated by decentralized peer nodes and associated with a DID Namespace. Preferably built on Hyperledger Indy, this [DID Ledger](#), is governed by an independent governing body and its own governance framework. Due to the overuse of terms such as "Network" and "Ledger", the term "Utility" has been accepted by the Bedrock Consortium to allow for additional clarity. See also *Backbone Network*.

Remote Identity Utility (Remote IUN)

An Identity Utility Network associated with a DID Root Namespace that operates under its own Governance Framework.

Decentralized DID Namespace Registry (DDNR)

Provides registration, discovery, and access for an Identity Utility Network.

Identity Utility Administrator

See *Utility Service Provider*

Utility Service Provider

The provider of operational and maintenance services for an Identity Utility Network.

Trustee

An Identity Owner entrusted with specific identity control responsibilities by another Identity Owner or with specific governance responsibilities by a Governance Framework. See *Recovery Key Trustee*

Consortium Trustee

A Trustee who is a member of the Bedrock Consortium Board of Directors. The trust in Consortium Trustees is bestowed collectively on behalf of all Identity Owners.

Key Recovery

The process of recovering access to and control of a set of Private Keys—or an entire Wallet—after loss or compromise. Key Recovery is a major focus of the emerging DKMS standard for cryptographic key management. See also *Recovery Key*.

Recovery Key

A special Private Key used for purposes of recovering a Wallet after loss or compromise. In the DKMS key management protocol, a Recovery Key may be cryptographically sharded for secret sharing among multiple Trustees.

Recovery Key Trustee

A Trustee trusted by another Identity Owner to authorize sharing back a Recovery Key for purposes of restoring a Wallet after loss or compromise.

Membership Management System

The means by which the Governing Board tracks membership entitlements and status. This MAY be implemented via a Salesforce tenant operated by the Linux Foundation with custom hooks into the Bedrock Business Utility.

Digital Trust Ecosystem

An interdependent group of enterprises, people and/or things that share a standardized trust model for mutually beneficial purposes, such as consumer and commercial interactions that are verifiable.

CLI Private Key

The Private-Key used by a Steward when interacting with the Indy CLI.

Validator Private Key

The Private-Key used by the Validator Node when performing concensus.

Governing Bodies

Governing Bodies

This is a Controlled Document of the Bedrock Governance Framework was approved by the Bedrock Consortium Board of Directors.

Document Name	Bedrock Governing Bodies
Version	v0.9
Approval Date	
Status	Pre-Launch Phase: Governance Framework Development
Governs	Governance bodies within the Bedrock Consortium
Governed By	Bedrock Consortium Governing Board

This document lists all official governing bodies of the Bedrock Consortium Foundation as determined by the Bedrock Consortium Board of Directors.

NOTE This document is pending resolution to [Issue 19](#).

Preface

1. All Bedrock Consortium Governing Bodies operate under the Bedrock Consortium Governing Body Policies.
2. By default, all Governing Bodies will leverage the Wiki assigned by the [Linux Foundation Groups Collaboration Tool](#). See [Issue 18](#)
3. For access to the current membership roster, meeting information, agenda, and the minutes of any Bedrock Consortium Governing Body, follow the link to its meeting page.

4. Unless otherwise noted, membership in any governing body is limited to BBU members in good standing.

Governing Board

The Bedrock Consortium Governing Board is the overall governing body of the Bedrock Consortium Foundation. It is chartered by the Bedrock Business Utility Fund as stated in the Participation Agreement. The Governing Board is composed of **Governing Members** who have the obligation to represent the interests of the Identity Owners of the Bedrock Consortium Community. It has sole authority for:

1. Approving the charters of all Bedrock Consortium Governing Bodies.
2. Approving at least one chairperson of each Bedrock Consortium Governing Body.
3. Approving new versions of the BBU Governance Framework.
4. Approving new versions of each Controlled Document.
5. **Charter Location:** [Participation Agreement \(MS-WORD\)](#)

Technical Steering Committee (TSC)

The Technical Steering Committee is responsible for the technical design, architecture, and policies governing Bedrock Consortium Infrastructure. Membership in this committee is open for all but it should be comprised of representatives from the Consortium members. The Chair of this committee MUST be a representative of the Steward community.

- **Charter Version:** xx
- **Charter Approval Date:** 2020-xx-xx
- **Charter Location:** [Technical Steering Committee Charter](#)
- **Meeting Page Location:** [Technical Steering Committee Meeting Page](#)

Governing Board Subgroups

Excluding the TSC, all Committees and Working Groups are governed by and fall under the the Governing Board.

Membership Committee

The Chair of this committee MUST be a representative of the Steward community.

The Membership Committee has the following responsibilities:

1. Communications amongst members
2. Membership campaigns to keep membership numbers stable for sustainability
3. Gathering and synthesizing feedback from members for consumption by the BoD.
4. **Charter Version:** xx
5. **Charter Approval Date:** 2020-xx-xx
6. **Charter Location:** [Membership Committee Charter](#)
7. **Meeting Page Location:** [Membership Committee Meeting Page](#)

Finance Committee

The Chair of this committee MUST be a representative of the Steward community.

The Finance Committee has the following responsibilities:

1. Budget Management
2. Utility Service Provider Bid Process
3. **Charter Version:** xx
4. **Charter Approval Date:** 2020-xx-xx
5. **Charter Location:** [Finance Committee Charter](#)
6. **Meeting Page Location:** [Finance Committee Meeting Page](#)

MarComm Committee

The Marketing and Communications ("MarComm") Committee is responsible for assisting the Governing Board in fulfilling marketing and external communication activities.

- **Charter Version:** xx
- **Charter Approval Date:** 2020-xx-xx
- **Charter Location:** [MarComm Committee Charter](#)
- **Meeting Page Location:** [MarComm Committee Meeting Page](#)

Governance Framework Working Group

The Bedrock Governance Framework Working Group (BGFWG) is responsible for development and revision of the BBU-GF. The Chair of this working group MUST be a representative of the Steward community.

- **Charter Version:** xx
- **Charter Approval Date:** 2020-xx-xx
- **Charter Location:** [Governance Framework Working Group Charter](#)
- **Meeting Page Location:** [Governance Framework Working Group Meeting Page](#)

Bedrock Consortium Bylaws

Bedrock CONSORTIUM AMENDED AND RESTATED BYLAWS – NEED LEGAL
INSIGHT

Issue 32

ARTICLE I. NAME OF CORPORATION

The name of the corporation is Bedrock Consortium (“Corporation”).

ARTICLE II. CORPORATE PURPOSE

The general and specific purposes of the Corporation are set forth in the Articles of Incorporation.

ARTICLE III. MEMBERSHIP

The Corporation shall have no members for purposes of the Utah Revised Nonprofit Corporation Act. The term “members” may be used in these Bylaws and in other corporate documents to refer to donors, technology contributors, ledger stewards, members of Corporation committees or work groups, and other participants in the Sovrin community whose roles may be further defined in the Bylaws, agreements, or other governing documents.

ARTICLE IV. Board of Directors

Section 1. General Powers

For purposes of the Utah Revised Nonprofit Corporation Act, the use of the term “Trustee” is intended to include all the powers and responsibilities of a director under the statute. The affairs of the Corporation shall be managed by its Board

of Directors. The Board of Directors shall have control of and be responsible for the management of the affairs and property of the Corporation.

Section 2. Number, Election, Tenure and Nominations

1. Number. The number of Trustees shall be fixed from time to time by the Trustees but shall consist of no less than three (3) nor more than twenty-one (21) persons. The Chairs of TGB Council and I4A Council shall be ex-officio members with all the rights of other board members.
2. Election. The initial Board of Directors is established by the Articles of Incorporation (the "Initial Trustees"). Trustees up for election shall be elected at the annual meeting upon the affirmative vote of a majority of Trustees present, provided that a quorum exists as provided in Section 7 of this Article IV. The members of the Board of Directors shall, upon election, immediately commence to perform their duties and shall continue in office until their successors shall be duly elected and qualified.
3. Tenure. The Initial Trustees shall serve for a term of 18 months. Thereafter, newly elected members of the Board of Directors who have not served before shall serve initial one-year terms. At the conclusion of a Trustee's initial term, the Trustee is eligible to be considered for re-election to a term of one to three years, staggered in order to ensure future orderly transition on the Board. Nominees recommended by the nominating committee may volunteer for the newly staggered terms for the first election. If the staggered terms are not evenly distributed, then the Executive Committee will assign Trustees to terms to make them evenly staggered. Newly added members of the Board of Directors shall serve until the next regularly scheduled election unless the resulting term would be less than six months in which case they would serve until the second regularly scheduled election and then if eligible for an additional term, that term will be set by the Executive Committee to correspond to the already staggered terms of the Board of Directors as to ensure an even amount of staggered terms going forward.
4. Nominations. Prior to the completion of the initial Trustees term and annually thereafter, the Board shall select a nominations committee to present a list to the Board of Trustees containing names of eligible nominees as Trustees for the ensuing year. Said list shall contain the names of at least

one eligible nominee to each vacancy. In case the Board of Trustees fails, for any reason, to elect such a committee within the time specified, then it shall be the duty of the Chair to appoint such a committee. Nominations made by the committee for the Trustees must be delivered to the Secretary at least thirty (30) days before the completion of the initial Trustees term and annually thereafter. The Secretary shall attach a list of nominees to the notification of the March meeting of the Board of Directors annually.

Section 3. Regular and Annual Meetings

An annual meeting of the Board of Directors shall be held at a time and day in the month of March of each calendar year and at a location designated by the Board. The Board of Directors may provide by resolution the time and place, for the holding of regular meetings of the Board. Notice of the annual meeting, and notice of the first regular meeting under a Board resolution, shall be sent in writing or electronically to all members of the Board of Directors no fewer than ten (10) days prior to the meeting date, subject to waiver of notice as provided in the Utah Revised Nonprofit Corporation Act.

Section 4. Special Meetings

Special meetings of the Board of Directors may be called by or at the request of the Chairperson or any two members of the Board of Directors. The person or persons authorized to call special meetings of the Board of Directors may fix any location as the place for holding any special meeting of the Board called by them but must give the other Trustees notice at least two (2) days in advance of the meeting by telephone, electronically, or in writing, subject to waiver of notice as provided in the Utah Revised Nonprofit Corporation Act. The meeting notice need not specify the purpose of the meeting.

Section 5. Participation in Meetings

Any Trustee may participate in an annual, regular, or special meeting of the Board of Directors, or conduct such a meeting, through the use of any means of communication by which all participating Trustees may hear each other during the meeting or, in the case of hearing impaired persons, read the other Trustees'

remarks during the meeting. Trustees participating by such means shall be counted as "present" for quorum purposes and may participate in discussion and voting.

Section 6. Action without Meeting

Any action required or permitted to be taken at a meeting of the Board of Directors may be taken without a meeting, provided there is written notice (which may be electronic) to all Trustees at least two (2) days in advance and no Trustee objects within the notice period to the action being taken without a meeting. The proposed action is approved only if it receives the requisite number of affirmative votes in writing (which may be electronic) under the applicable quorum and voting requirements herein.

Section 7. Quorum

The presence of a simple majority of current members of the Board of Directors shall be necessary at any meeting to constitute a quorum to transact business, but a lesser number shall have power to adjourn to a specified later date without notice. The act of a majority of the members of the Board of Directors present at a meeting at which a quorum is present shall be the act of the Board of Directors, unless the act of a greater number is required by law or by these Bylaws.

Section 8. Forfeiture

Any member of the Board of Directors who fails to attend three Board meetings in three consecutive calendar months shall automatically forfeit his or her seat on the Board, unless a majority of the other Trustees vote to retain the Trustee in question. The Secretary shall notify the Trustee in writing that his or her seat has been declared vacant, and the Board of Directors may immediately proceed to fill the vacancy.

Section 9. Vacancies

Whenever any vacancy occurs in the Board of Directors it shall be filled without undue delay by a majority vote of the remaining members of the Board of

Directors. Vacancies may be created and filled according to specific methods approved by the Board of Directors.

Section 10. Compensation

Members of the Board of Directors shall not receive any compensation for their services as Trustees, but they may be reimbursed for expenses incurred on behalf of the Corporation, subject to approval by the Board.

Section 11. Confidentiality

Trustees shall use discretion and good judgment in discussing the affairs of the Corporation with third parties. Trustees shall not disclose to third parties any trade secrets, confidential commercial information, personally identifiable information, or other nonpublic information that has been acquired by the Corporation or shared with the Corporation under conditions of confidentiality, except as required by law. Trustees may be required to execute a confidentiality agreement as a condition of appointment to the Board of Directors.

Section 12. Advisory Councils

The Board of Directors may create Advisory Councils (such as a Trust Framework Committee and a Technical Governance Committee) whose members shall be elected by the Board of Directors annually but who shall have no duties, voting privileges, nor obligations for attendance at regular meetings of the Board.

Advisory Council members may attend Board meetings at the invitation of a Trustee. Otherwise, members of Advisory Councils shall function according to a charter approved by the Trustees, with the purpose of supporting the Sovrin community and the work of the Corporation. Members of Advisory Councils may be required to sign confidentiality and intellectual property agreements and to comply with committee procedures approved by the Board.

Section 13. Parliamentary Procedure

Any question concerning parliamentary procedure at meetings shall be determined by the Chairperson by reference to Robert's Rules of Order Newly Revised.

Section 14. Removal.

Any member of the Board of Directors or members of the Advisory Council may be removed with or without cause, at any time, by the vote of three-quarters (3/4) of the members of the Board of Directors if in their judgment the best interest of the Corporation would be served thereby. Each member of the Board of Directors must receive written (including electronic) notice of the proposed removal at least ten (10) days in advance of the proposed action. An officer who has been removed as a member of the Board of Directors shall automatically be removed from office.

ARTICLE V. OFFICERS

The officers of this corporation shall be the Chairperson, Vice-Chair, Secretary and Treasurer. A single Trustee may serve as both Secretary and Treasurer. All officers must be current Trustees.

Section 1. Chairperson

The Chairperson shall preside at meetings of the Board of Directors and the Executive Committee. The Chairperson shall have general oversight of all Corporation planning, activities, finances, staff, contractors, and records. The Chairperson shall have the authority to execute agreements on behalf of the Corporation. The Chairperson shall be ultimately responsible for relations between the Corporation, stewards, technology developers, users, donors, and other members of the Sovrin community.

Section 2. Vice-Chair

The Vice-Chair shall be vested with all the powers and shall perform all the duties of the Chairperson during the absence of the latter. The Vice-Chair shall discharge such other tasks as may be delegated to him or her by the Board of Directors.

Section 3. Secretary

The Secretary shall provide notices and make records of all meetings of the Board of Directors and the Executive Committee and ensure that Corporation documents are made available to Trustees and other relevant persons. The Secretary shall advise the Chairperson on parliamentary rules of procedure as required. The Secretary shall record attendance and voting at meetings and in Board actions without meeting. The Secretary shall assist the Chairperson and supervise Corporation staff in communicating with the Sovrin community and third parties. The Secretary shall ensure that required federal and state reports are submitted in a timely manner to maintain the Corporation's tax-exempt status.

Section 4. Treasurer

The Treasurer shall maintain books of account and bank records for the Corporation and oversee the Corporation's fundraising activities. The Treasurer shall retain and supervise an independent accountant and ensure that required financial and tax reports are prepared and submitted.

Section 5. Election of Officers

The Board of Directors shall elect officers at its annual meeting or at a regular or special meeting of the Board. Officers shall serve for a term of one (1) year, although the Board may extend the term to end at the next annual meeting. An individual may be reelected for no more than three successive terms.

Section 6. Removal of Officer

An officer may be removed from office, while continuing to serve on the Board of Directors, if at least two thirds (2/3) of the other Trustees vote to remove the Trustee from office. The Board may then elect a successor for the remainder of the officer's term. A vote to remove an officer may only be taken after giving the officer an opportunity to be heard following at least ten (10) days' written (including electronic) notice of intent to move for the officer's removal at a regular or special meeting of the Board of Directors, with a summary of the reasons for such a motion.

Section 7. Vacancies

The Board of Directors may also appoint successors to fill vacancies that otherwise occur in offices, such persons serving for the unexpired term of the office.

ARTICLE VI. COMMITTEES

Section 1. Committee Formation

The Board of Directors may create Advisory Councils and other committees as needed. The Board approves committee charters and appoints all committee chairs and budgets.

Section 2. Executive Committee

The Officers automatically constitute the Executive Committee of the Board. The Board of Trustees may elect additional Trustees to serve on the Executive Committee. The Executive Committee is responsible for the day-to-day management of the Corporation within the policy guidelines established by the Board of Directors, which may also assign specific tasks to the Executive Committee by Board resolution. Except for the power to amend the Articles of Incorporation and Bylaws, the Executive Committee shall have all the powers and

authority of the Board of Directors in the intervals between meetings of the Board of Directors, and is subject to the direction and control of the full Board.

Section 3. Finance Committee

The treasurer is the chair of the Finance Committee, which shall include two other Trustees appointed by the Board. The Finance Committee is responsible for developing and reviewing fiscal procedures, fundraising plans, and the annual budget with staff and other Trustees. The budget must be approved by the Board, and all expenditures must be within budget. Any material change in the budget must be approved by the Executive Committee or the full Board. The fiscal year shall be the calendar year. Annual reports are required to be submitted to the Board showing income, expenditures, and pending income. The financial records of the Corporation, as a tax-exempt nonprofit, are expected to be made available to the Sovrin community and to the public.

ARTICLE VII. CORPORATE STAFF

It is anticipated that the Corporation will have professional staff, either as direct employees or through a management firm.

Section 1. Executive Director

The Board of Directors may hire or contract for an Executive Director who shall serve at the will of the Board. The Executive Director shall have immediate and overall supervision of the operations of the Corporation, and shall direct the day-to-day business of the Corporation, maintain the properties of the Corporation, hire, discharge, and determine the salaries and other compensation of all staff members under the Executive Director's supervision, and perform such additional duties as may be directed by the Executive Committee or the Board of Directors. No officer, Executive Committee member or member of the Board of Directors may individually instruct the Executive Director or any other employee without the consent of the Executive Committee or the Board of Directors. The Executive Director shall make such reports at the Board and Executive Committee meetings as shall be required by the Chairperson or the Board. The Executive Director shall

be an ad-hoc member of all committees. The Executive Director may not be related by blood or marriage/domestic partnership within the second degree of consanguinity or affinity to any member of the Board of Directors or Advisory Council. The Executive Director may be hired at any meeting of the Board of Directors by a majority vote and shall serve until removed by the Board of Directors by majority vote of a quorum present at any meeting of the Board Trustees. Such removal may be with or without cause. Nothing herein shall confer any compensation or other rights on any Executive Director, who shall remain an employee terminable at will, as provided in this Section.

Section 2. Other Staff

The Executive Director may make recommendations to the Board for the hiring or contracting of other staff members. ARTICLE VIII. CONFLICT OF INTEREST AND COMPENSATION The Trustees shall be subject to a Conflict of Interest Policy adopted by the Board of Directors and which shall be attested to annually by each Trustee. ARTICLE IX. LIABILITY AND INDEMNIFICATION Section 1. Nonliability of Trustees and Officers To the extent permissible under Utah and federal law, trustees and officers shall not be held personally liable for the debts, liabilities, or other obligations of the Corporation. Section 2. Indemnification To the full extent permitted under the laws of the State of Utah, the Corporation shall indemnify any current or former trustee, officer, employee, or agent of the Corporation (each referred to in this Article as an “indemnitee”) against expenses actually and necessarily incurred by such indemnitee in defending against any action, suit, or proceeding in which that indemnitee is made a party by reason of being or having been a trustee, officer, employee, or agent of the Corporation, except to the extent that the indemnitee is adjudged liable for negligence or misconduct in the performance of a duty for the Corporation. The foregoing indemnification shall not be deemed exclusive of any other rights to which an indemnitee may be entitled under any By-Law, agreement, resolution of the Board of Directors, or otherwise.

Section 3. Expenses

Expenses (including reasonable attorneys' fees) incurred in defending a civil or criminal action, suit, or proceeding may be paid by the Corporation in advance of

the final disposition of such action, suit, or proceeding, if authorized by the Board of Directors, upon receipt of an undertaking by or on behalf of the indemnitee to repay such amount if it shall ultimately be determined that such indemnitee is not entitled to be indemnified hereunder.

Section 4. Insurance

The Corporation may purchase and maintain insurance on behalf of any person who is or was a trustee, officer, employee, or agent against any liability asserted against such person and incurred by such person in any such capacity or arising out of such person's status as such, whether or not the corporation would have the power or obligation to indemnify such person against such liability under this Article.

ARTICLE X. BOOKS AND RECORDS

The Corporation shall keep complete books and records of account and minutes of the proceedings of the Board of Directors. These may be kept in electronic form.

ARTICLE XI. AMENDMENTS

Section 1. Articles of Incorporation

The Articles of Incorporation may be amended at any regular or special meeting of the Board of Trustees, or by action of the Board of Directors without meeting, by the affirmative vote of a majority of all Trustees, provided that the text of the proposed amendment is furnished to each Trustee at least five (5) days in advance of such a meeting.

Section 2. Bylaws

The Board of Directors may amend these Bylaws by majority vote of a quorum present at any regular or special meeting of the Board, or by action of the Board of Directors without meeting, provided that the text of the proposed amendment

or a summary of the proposed changes is furnished at least five (5) days in advance. The text may be modified in the course of the debate at the meeting and adopted by a majority vote without requiring notice of a further meeting.

ADOPTION OF AMENDED AND RESTATED BYLAWS

These Amended and Restated Bylaws were ADOPTED AND APPROVED unanimously by the Board of Directors on this XXst day of January, 2020.

xxxxxxxxxxxxxx, Chairperson

xxxxxxxxxxxxxx, Secretary

Governing Body Policies

Governing Body Policies

This is a Controlled Document of the Bedrock Governance Framework was approved by the Bedrock Consortium Board of Directors.

Document Name	Bedrock Consortium Governing Body Policies
Version	
Approval Date	
Status	Pre-Launch Phase: Governance Framework Development
Governs	Chartering, Types and Membership, Chairpersons, Facilitators, Voting, Self-Organization, Meetings, and Meeting Pages
Governed By	Bedrock Consortium Governing Board

NOTE: * See [Issue 17](#) * See [Issue 20](#)

1. Chartering

1. The organizers of a new Bedrock Consortium Governing Body MUST submit a charter to the Bedrock Consortium Governing Board.
2. The charter MUST be based on the Bedrock Consortium Governing Body Charter Template maintained by the Secretary of the Bedrock Consortium BoD.
3. This template MUST include:
 - a. Version number and date of approval.
 - b. General Policies.

- c. Status (see Types and Membership, below).
 - d. Purpose.
 - e. Principles (if any beyond the Core Principles).
 - f. Activities and Duties.
 - g. Membership.
 - h. Chairperson(s).
 - i. Facilitator(s).
 - j. Voting.
 - k. Funding.
 - l. Meeting Schedule.
 - m. Meeting Page.
 - n. Version History.
4. The version history MUST include the version numbers, dates, and links to all previous versions of the charter.
 5. After the required public review period (see Bedrock Consortium Governance Framework V2 Master Document section 4.3), a new or revised charter MUST be approved by the Bedrock Consortium Governing Board before it becomes active.
 6. Once approved, information about the new or revised Bedrock Consortium Governing Body MUST be added to:
 - a. The Bedrock Consortium Governing Bodies Controlled Document, including all the information required therein.
 - b. The Bedrock Consortium Foundation website.

2. Types and Membership

1. A Bedrock Consortium Governing Body MUST be one of the following types:
 - a. Council.
 - b. Committee.
 - c. Working Group.
2. All Bedrock Consortium Governing Bodies MUST:

- a. Have at least one and MAY have up to three chairpersons, either appointed by the Bedrock Consortium Governing Board or elected by their members.
 - b. Have at least three members, including the chairperson(s).
 - c. State any other specific membership requirements in its charter.
3. A council: a. MUST have at least one chairperson appointed by the Bedrock Consortium Governing Board who, if not already a Trustee, shall serve as an ex-officio Trustee unless an exception is made by the BoD. b. MAY limit the total number of voting members. c. MAY establish membership term limits.
4. A committee: a. SHOULD have a Trustee serving as at least one of its chairperson(s).
b. MAY limit the total number of voting members. c. MAY establish membership term limits.
5. A working group:
a. MUST be open to participation by any member of the Bedrock Consortium Community. b. MUST NOT establish membership term limits.

3. Chairpersons

- 1. A chairperson of a Bedrock Consortium Governing Body: a. MUST be a member of that Bedrock Consortium Governing Body.
b. MUST NOT be an employee of the Bedrock Consortium Foundation unless an exception is made by the BoD. c. SHOULD NOT be a chairperson of another Bedrock Consortium Governing Body.
- 2. If a Bedrock Consortium Governing Body has more than one chairperson, they MUST NOT be affiliated with the same organization.

4. Facilitators

- 1. A Bedrock Consortium Governing Body MAY have one or more facilitators.
- 2. It is NOT REQUIRED for a facilitator to be a member of that governing body.
- 3. An employee of the Bedrock Consortium Foundation MAY serve as a facilitator.

5. Subgroups

1. In keeping with the Decentralization by Design Principles (section 2.8 of the Bedrock Consortium V2 Master Document), and in particular the Distributive principle (section 2.8.7), all Bedrock Consortium Governing Bodies SHOULD self-organize and delegate work to subgroups as much as possible.
2. A Bedrock Consortium Governing Body MAY appoint the following types of subgroups as needed to accomplish its mission: a. Team – an ongoing subgroup organized around a focus area. b. Task Force – a short-term subgroup organized to accomplish a specified task within a specified time period.
3. An organized subgroup of a Bedrock Consortium Governing Body MUST be listed on its meeting page together with information about how to participate in that subgroup.
4. An organized subgroup SHOULD maintain its own meeting page separate from but linked from the governing body's main meeting page.

6. Funding

1. A Bedrock Consortium Governing Body MAY request a specified level or type of funding in its charter.
2. A Bedrock Consortium Governing Body MAY make a special request for funding to engage outside professionals or other external resources to assist in their work provided any financial compensation is approved by the Bedrock Consortium Foundation Executive Director.

7. Voting

1. All Bedrock Consortium Governing Bodies SHOULD strive to reach decisions by consensus.
2. Consensus MAY be achieved via discussion at a web-meeting or face-to-face meeting or via any online mechanism, such as a mailing list, that provides

adequate notice to all members and enables any member to lodge an objection and request a formal vote.

3. When a formal vote is required, it MUST be conducted using a voting process agreeable to the majority of the group, or if such an agreement cannot be reached, then under Roberts Rules of Order, Newly Revised , 11th Edition, ISBN 978-0-306-82021-2.
4. If members feel that a decision has been reached improperly, they may appeal the decision to the Bedrock Consortium Governing Board who MUST serve as the final authority in all disagreements.

8. Intellectual Property Rights

1. In keeping with the mission of the Bedrock Consortium Foundation as an open public trust organization, all contributions by participants in a Bedrock Consortium Governing Body MUST be free of intellectual property rights or other usage restrictions.
2. Excluding explicit contributions as defined in 8.1, participants in a Bedrock Consortium Governing Body retain all rights to their existing intellectual property and participation in a Bedrock Consortium Governing Body MUST NOT be construed as a license to any existing intellectual property rights.

9. Meetings

1. In keeping with the Transparency Principle (Bedrock Consortium V2 Master Document section 2.6), Bedrock Consortium Governing Bodies:
 - a. MUST conduct open, transparent meetings with the exception of special closed sessions.
 - b. MUST only conduct special closed sessions (not open to the public) when the group needs to deal with matters where confidentiality is required due to:
 - a. Legal regulations.
 - b. Security concerns (breach responses, confidential procedures, etc.).
 - c. Steward concerns (policy violations, business transitions, etc.)
 - d. Discrimination, harassment, or other human resource matters.

- e. Other matters where confidentiality is advised by Bedrock Consortium Foundation legal counsel.
- c. SHOULD conduct meetings that allow virtual participation whenever possible.

10. Meeting Pages

- 1. All Bedrock Consortium Governing Bodies MUST maintain a meeting page based on the Bedrock Consortium Governing Body Meeting Page Template .
- 2. A link to the meeting page for a Bedrock Consortium Governing Body MUST be included in the listing in the Bedrock Consortium Governing Bodies Controlled Document and on the Bedrock Consortium Foundation website.
- 3. The meeting page MUST include:
 - a. All information about the group listed in Bedrock Consortium Governing Bodies , including a link to the current charter.
 - b. A list of the current chairperson(s).
 - c. A list of the current facilitator(s).
 - d. A list of current active members.
 - e. Information about how to join the group.
 - f. Information about any organized subgroups, including:
 - a. The name and purpose of the subgroup.
 - b. Membership requirements.
 - c. Instructions on how to participate.
 - d. A link to the subgroup's meeting page, if applicable.
 - g. A schedule of open public meetings.
 - h. Information about how to participate in open public meetings (physical or virtual).
 - i. Information about how to participate in open public chat channels (e.g., Rocketchat).
 - j. Agendas and meeting minutes/notes listed in reverse chronological order.
 - k. Links to any archived versions of the meeting page.
- 4. The minutes or notes of each meeting MUST be recorded on or linked to the meeting page.
- 5. The meeting page SHOULD be periodically archived to prevent it from growing too large.

11. Reporting

1. All Bedrock Consortium Governing Bodies:
 - a. SHOULD designate a member to attend and give a monthly report to the Bedrock Consortium BoD.
 - b. MUST submit a monthly summary report of activity to the Bedrock Consortium Governing Board via either:
 - a. An oral report given during the monthly Governing Board meeting with a written summary added to the Governing Board Meeting Page.
 - b. A written report added to or linked to the Governing Board Meeting Page
 - c. SHOULD send the same monthly report to the Steward mailing list.
2. The Secretary of the Bedrock Consortium Governing Board MAY request oral or written reports as needed.

Ledger Access Policies

This is a Controlled Document of the Bedrock Governance Framework was approved by the Bedrock Consortium Board of Directors.

Document Name	Bedrock Consortium Ledger Access Policies
Version	v0.9
Approval Date	
Status	Pre-Launch Phase: Governance Framework Development
Governs	Policies for reading and writing to the Bedrock Business Utility
Governed By	Bedrock Governance Framework Workgroup

1. Declaration of Intent

The Bedrock Business Utility (the "Utility") will operate with limited write access as specified by the Permissioned Write Access processing section declared herein.

The scope of these policies pertains to the full corpus of **Utility Environments**, namely all the ledgers associated with the Bedrock Business Utility (i.e.: prod, test, dev).

2. Recommended Reading

The terms used in this Controlled Document are more fully explained in the [Glossary](#), as well as in the [Legal Architecture Overview](#) which includes a visual diagram.

One topic pertinent to ledger access is the concept of a [Tombstone](#). A Steward MAY, for regulatory or individual business requirements, determine that it needs to forbid access to a ledger entry and therefore require the ability to mark the subject entry as "deleted". While the Bedrock Consortium has taken action to minimize such risk by prohibiting public write access, a *Tombstone* provides an added protection mechanism that will help mitigate risk for Stewards who are contractually obligated to carry out read and write transactions.

The Utility will allow for Tombstones once this feature is implemented in Hyperledger Indy. The Bedrock Consortium will collaborate with the Hyperledger Indy Community and the [Bedrock Consortium Project](#) (the "Technical Project") to allow a Steward to:

1. Mark a Transaction as "deleted" thereby suggesting it should no longer be returned in response to requests for read access.
2. Declare a Transaction as "deleted" under one of two categories: *Node-Specific Tombstone* or a *Ledger-Wide Tombstone*.

Tombstones do not modify data on the ledger. Instead they impact the behavior of a Steward Node that serves data from the ledger. In the general, a Tombstone MAY be used by a Steward that is forced to comply with a legal demand to stop returning a specific Transaction, such as a Transaction containing data that is locally considered Personal Data or that is illegal or violates the Transaction Author Agreement in some other way. In such a case, other Stewards may not face the same legal demands and may take different action.

1. Transaction Author Agreement

1. The Bedrock Consortium MUST:
 - a. Publish a Transaction Author Agreement between a Transaction Author and the Bedrock Consortium (representing the Bedrock Business Utility as a whole) specifying the terms and conditions under which Transaction Authors agree to submit write Transactions to the Utility, including the policies defined in this Controlled Document.
 - b. Publish a Steward Data Processing Agreement (DPA) specifying the requirements for a Steward to serve as a Data Processor on behalf of

Transaction Authors as Data Controllers and the Bedrock Consortium as a Designated Data Controller.

- c. When necessary, revise the Transaction Author Agreement and the Steward DPA under the same policies as a Controlled Document as specified in the [Governance](#) section of the Bedrock Governance Framework Master Document.
 - d. Maintain a published version of the Transaction Author Agreement and the Steward DPA in the [Bedrock Consortium Code Repository](#).
2. A Transaction Author MUST agree not to submit Transactions that contain:
- a. Data that would violate the intellectual property rights of others.
 - b. Data that may not lawfully be written to the Utility, where the definition of applicable law in this context is provided in the Transaction Author Agreement.
3. A Transaction Author MUST agree not to submit a Transaction that contains Personal Data.
4. A Transaction Author MUST agree that if it is determined in a court of law that one or more Transactions made by the Transaction Author violated the terms and conditions of the Transaction Author Agreement, the Transaction Author consents to the marking of those Transactions with a Tombstone and, if possible, the revocation of the State Proof(s) pertaining to the Utility data for those Transactions.

2. Transaction Endorser Agreement

1. The Bedrock Consortium MUST:
- a. Publish a Transaction Endorser Agreement between the Transaction Endorser and the Bedrock Consortium specifying the terms and conditions under which Transaction Endorsers agree to write Transactions to the Utility, including the policies defined in this Controlled Document.
 - b. Publish a Transaction Endorser Data Processing Agreement (DPA) specifying the requirements for a Transaction Endorser to serve as a

Data Processor on behalf of Transaction Authors as Data Controllers and the Bedrock Consortium as a Designated Data Controller.

- c. When necessary, revise the Transaction Endorser Agreement and the Transaction Endorser DPA under the same policies as a Controlled Document as specified in the [Governance](#) section of the Bedrock Governance Framework Master Document.
 - d. Publish the current version of the Transaction Endorser Agreement and the Transaction Endorser DPA in the [Bedrock Consortium Code Repository](#).
2. A Transaction Endorser MUST adhere to membership entitlements that constrain the number of transactions that may be submitted as specified in the Transaction Endorser Agreement.
 3. A Transaction Endorser MUST:
 - a. Only submit Transactions from Transaction Authors who have explicitly agreed to the Transaction Author Agreement by physically signing a copy.
 - b. Maintain physical or digital evidence of conformance to this policy.

3. Permissioned Write Access

1. The scope of the policies defined in this section is defined as follows:
 - a. The policies in this section MUST apply to all Utility Environments.
 - b. The policies governing write access to non-production Utility Environments (i.e.: Dev, Test) MAY be defined separately by other Controlled Documents.
2. Bedrock Consortium Trustees are permitted to write Transactions to the Utility under the following rules:
 - a. This policy MUST apply only to Trustees acting in their role as Trustees of the Bedrock Consortium.

- b. A Trustee MUST only make the following Transactions if the Transaction has been approved by a motion of the Bedrock Consortium Board of Directors.
 - i. Add or remove a Trustee.
 - ii. Add or remove a Steward.
 - iii. Add or remove a Transaction Endorser.
 - iv. Update or receive updates from the Membership Management System.
 - c. A Trustee MAY make Utility maintenance Transactions if the Transaction is approved by either the Bedrock Consortium Board of Directors.
3. Bedrock Consortium members who are permitted to serve in the role of Transaction Endorsers MUST agree to the Transaction Endorser Agreement by submitting a physically or digitally signed copy to the Bedrock Consortium.
4. Transaction Authors are permitted to write Transactions to the Utility provided::
- a. Each Transaction includes a valid digital signature from the Transaction Author.
 - b. The Transaction is endorsed by an approved Transaction Endorser.
 - c. If the Transaction updates the state of a ledger-persisted data structure, it MUST be digitally signed by the same Transaction Author that recorded the previous state.

4. Public Write Access

- 1. Public Write Access is PROHIBITED.
- 2. All Utility Environments MUST adhere to Permissioned Write Access processing.

5. Public Read Access

1. The Utility MUST be publicly available for anyone to submit read transactions.
2. Stewards MUST provide public read access without cost for all Transactions on the Utility unless marked by a Tombstone.
3. Once Tombstone functionality has been:
 - a. implemented by the underlying ledger technology,
 - b. approved by the Sovrin Technical Steering Committee, and
 - c. approved by the Bedrock Consortium Board of Directors, a Steward MAY mark a Transaction as a Node-Specific Tombstone if:
 - i. Requested by the Transaction Author of a Transaction for a valid reason as specified by the Transaction Author Agreement.
 - ii. Required of the Steward by a court order.
 - iii. The Steward has evidence that the Transaction violates the terms and conditions of the Transaction Author Agreement.
4. A Steward MUST NOT use a Node-Specific Tombstone for any other reason.
5. Ledger-Wide Tombstones MUST NOT be implemented until policies governing their usage are published in a future version of this Controlled Document.

NOTE: Ledger-Wide Tombstones are not planned in the near future.

Ledger Data Policies

Ledger Data Policies

This is a Controlled Document of the Bedrock Governance Framework was approved by the Bedrock Consortium Board of Directors.

Document Name	Bedrock Ledger Transaction Data
Version	v0.9
Approval Date	
Status	Pre-Launch Phase: Governance Framework Development
Governs	Data and metadata processed by Nodes operated by Stewards in the course of completing a Transaction with the Bedrock Business Utility.
Governed By	Sovrin Technical Steering Committee

Ledger

This document assumes that Member Validator Nodes ("Nodes") are all running instances of [Hyperledger Indy](#) as the distributed ledger technology (DLT) that provides the underlying infrastructure for the Bedrock Business Utility ("the Ledger").

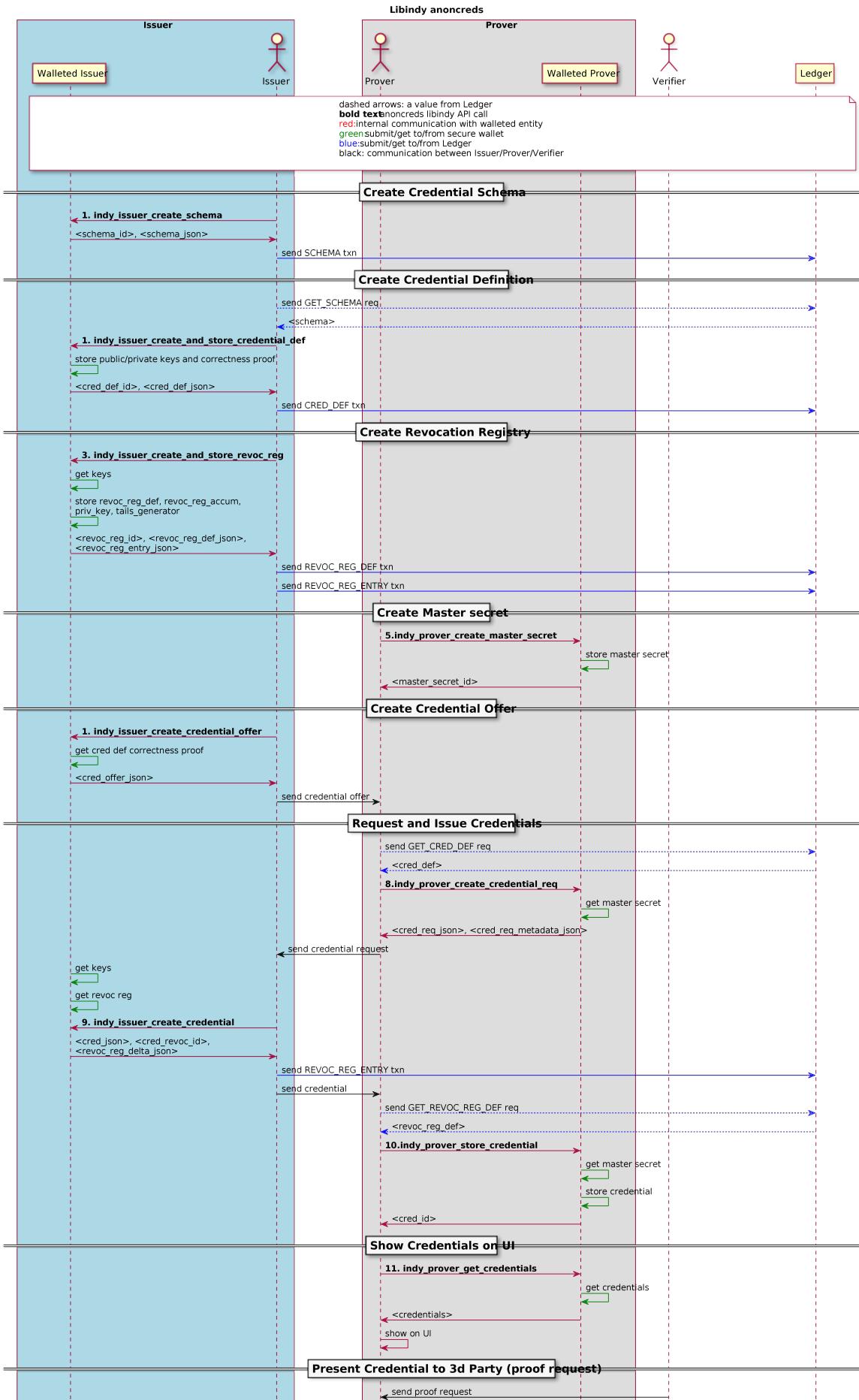
Transaction Data

Data and metadata processed by Nodes operated by Members in the course of completing a transaction with the Ledger governed By Bedrock Consortium will conform to the following requirements:

1. **Ledger Transaction Data Definitions:** Comply with the authoritative definitions for transaction data stored on the Ledger as outlined in Hyperledger Indy GitHub repository documents at the following locations:
 - a. General Transaction Information
 - b. Domain Ledger Transactions
 - i. NYM
 - ii. ATTRIB
 - iii. SCHEMA
 - iv. CLAIM_DEF
 - c. Pool Ledger Transactions
 - i. NODE
 - ii. Config Ledger Transactions
 - iii. POOL_UPGRADE
 - iv. NODE_UPGRADE
 - v. POOL_CONFIG
2. **Ledger Transaction Requests:** The authoritative definition of requests for Transactions with the Ledger are maintained in the following Hyperledger Indy GitHub repository document:
 - a. Ledger Node Requests

Anoncreds Workflow

The diagram below describes how and when data is written to the Ledger. For a detailed discussion pertaining to the processing of read and write transactions against the Ledger please refer to the [Anoncreds Workflow Process](#).



Member Business Policies

This is a Controlled Document of the Bedrock Governance Framework was approved by the Bedrock Consortium Board of Directors.

Document Name	Member Business Policies
Version	v0.9
Approval Date	
Status	Pre-Launch Phase: Governance Framework Development
Governs	Steward Qualification, Application, Activation, Operation, Notification, Suspension, Termination, and Transition
Governed By	Bedrock Governance Framework Work Group

1. Member Qualification

See [Issue 21](#) for review.

General

Prospective members MUST apply to the Governing Board and receive approval to be a Member of the Bedrock Consortium. See [Application process](#) herein.

Stewards

Prospective members seeking qualification under a membership type that is assigned the responsibility of running a utility infrastructure node MUST be:

1. A corporate member of The Linux Foundation.

2. A business entity that is identifiable with at least one of the following business verification services:

- a. [DUNS Number Lookup](#)
- b. [Legal Entity Identifier Lookup](#)

Subscribers

Prospective members seeking qualification as a Subscriber MUST be:

- 1. A corporate or affiliate member of The Linux Foundation.
- 2. An entity that meets one of the following criteria:
 - a. A business entity that is identifiable with at least one of the following business verification services:
 - i. [DUNS Number Lookup](#)
 - ii. [Legal Entity Identifier Lookup](#)
 - b. A governmental body or agency, or an entity predominantly owned and controlled by the state, in a Jurisdiction as defined in the [Glossary](#).
 - c. A governmentally regulated institution with at least five (5) years operating history.
 - d. A law firm, accounting firm, or other legally-regulated institution with at least five (5) years operating history.
 - e. A non-governmental organization (NGO) or Social Purpose Organization with at least five (5) years operating history.
 - f. An accredited university or other institution of higher education with at least five (5) years operating history.
 - g. A certificate authority (CA) with at least five (5) years operating history.

2. Application Process

See [Issue 22](#).

Prospective Member

To apply, an entity MUST submit a written application to the Membership Committee as directed on the Bedrock Consortium website.

Membership Committee

The committee MUST:

1. Ensure that all specific Practices and Procedures involved in the Member application process are publicly documented on the Bedrock Consortium website.
2. Ensure that Member application process follows the guidelines for Self-Certification, Certification, or Accreditation as specified by the Bedrock Consortium Trust Assurance Framework.
3. Ensure that the application form available upon request and minimally publicly documented on the Consortium's BBU-GF source control repo and/or website.
4. Notify the Linux Foundation of approved applications.
5. Notify applicants of application approval/rejection status.

Governing Body

The Governing Board MUST:

1. Take action on applications within 30 days of receipt.

3. Activation

Stewards

A Steward SHOULD submit a utility infrastructure node to the Identity Utility Administrator using the procedures outlined by the Technical Steering Committee after the following dependencies have been resolved:

1. Have their application approved by the responsible Bedrock Consortium Governing Body.
2. Complete the onboarding process with the Linux Foundation including the signature of all pertinent contractual instruments.

Before a Member may qualify to have an active Validator Node on the Utility, the Member MUST:

1. Pass any required tests on the Bedrock Consortium Test Network as specified by the Technical Steering Committee and documented in the Bedrock Consortium Code Repository.

After a Member has qualified to have an active Validator Node, the Member MUST designate the Utility environment(s) (e.g., prod, test, dev) which their Node may be activated.

1. The Member MUST make this designation following the procedures specified by the Technical Steering Committee.
 1. The Member MUST designate activation in at least one Utility environment.
 1. The Member MAY designate activation in more than one Utility environment.
 1. The Member MUST have at least one node designated for production.

4. Operation

1. A Member MUST operate its Node in compliance with the Member Technical and Organizational Policies.
2. A Member MUST requalify at least annually via the requalification process in effect at that point in time as specified by the responsible Bedrock

Consortium Governing Body and documented on the Bedrock Consortium website.

5. Notification

1. A Member MUST maintain current contact information for its business and technical points of contacts sufficient to ensure its staff are reachable in a timely manner.
2. A Member MUST notify the responsible Bedrock Consortium Governing Body if:
 - a. There is a change to the beneficial ownership of its Organization.
 - b. There is a change to the Member's legal name, trademark, or logo.
 - c. The Member changes the values of any of the Member's attributes submitted in the Member's original application, including legal jurisdiction, legal status, Node location, Node hosting type, or Node technical specifications, that are material to the Node Selection Algorithm.
 - d. There is any other substantial change to its Organization that impacts the qualification criteria in the Member Qualification section.
 - e. It suffers a data breach or other public event which may reasonably call into question its ability to comply with the Governance Framework.
3. In the case of any of the changes listed in #2 above, the responsible Bedrock Consortium Governing Body MAY require the Member to requalify.
4. The Bedrock Consortium MUST provide Members with at least 30 days notification of any material changes to the business policies implemented in Bedrock Consortium Network environments. Notification about technical changes is covered under Bedrock Consortium Member Technical and Organizational Policies .

6. Suspension

1. A Member MUST be suspended by the responsible Bedrock Consortium Governing Body under any of the following conditions:
 2. The Member no longer complies with the Member Business Policies, Member Technical and Organizational Policies, or any other requirements of the Bedrock Consortium Governance Framework.
 - a. The Member's Node has failed to achieve 98% availability over a period of 30 days.
 - b. A security intrusion or violation has been reported and the Technical Steering Committee is not satisfied that the Member has performed adequate remediation.
 - c. The Member fails to requalify under its annual requalification process specified in section 4.
 - d. The Member has, in the sole judgment of the Bedrock Consortium Board of Directors, violated some or all of the Governance Framework principles, taken action against the purpose of the Bedrock Consortium, or has shown behavior contrary to the collective interest of the Bedrock Consortium or performed action that brought the Bedrock Consortium or the Consortium into disrepute.
 3. A Member who is suspended MUST not have an active Node on any Bedrock Consortium Ledger network until such time as Member is able to provide reasonable assurance to the responsible Bedrock Consortium Governing Body that:
 - a. The Member is back in compliance with all requirements of the Bedrock Consortium Governance Framework, and
 - b. The Member has the ability to maintain compliance for the foreseeable future.
 4. At the request of a suspended Member, the responsible Bedrock Consortium Governing Body MUST examine the Member's remediation efforts and make one of the following decisions:
 - a. Reactivate the Member.

- b. Request further remediation by the Member.
- c. Terminate the Member.

7. Termination

- 1. A Member who has breached the terms of the Participant Agreement and/or associated Utility Agreements MAY be terminated by a majority vote of the responsible Bedrock Consortium Governing Body with ratification by the Board of Directors.
- 2. A Member who has been suspended and not been reactivated within 180 days following suspension MUST be notified of automatic termination.
- 3. An Organization who has been previously terminated as a Member and who applies to be reinstated MUST disclose the previous termination in their application and explain the remediation steps that the Member has taken to requalify.

Member Technical and Organizational Policies

This is a Controlled Document of the Bedrock Governance Framework was approved by the Bedrock Consortium Board of Directors.

Document Name	Member Technical and Organizational Policies
Version	v0.9
Approval Date	
Status	Pre-Launch Phase: Governance Framework Development
Governs	General Security Policies, Node Technical Policies, General Security Policies, Node Security Policies, Operating Policies, Node Selection Algorithm, Permissioned Test Network Policies, Reporting Policies
Governed By	Bedrock Governance Framework Work Group, Sovrin Technical Steering Committee

1. Ledger Software Policies

1. The Bedrock Board of Directors MUST decide the software technology and version used by all Nodes (Validator, Observer). This software is referred to as the *Bedrock Open Source Code*.
2. The Bedrock Board of Directors MUST require the TSC to establish best practices for continuous delivery and integration of the *Bedrock Open Source Code* using containerization.
3. The Bedrock Board of Directors MUST require the TSC and/or the Utility Service Provider to deploy an upgrade notification process that will allow Stewards to automatically recognize and act when upgrades are available.

4. The Bedrock Board of Directors MAY leverage the Technical Steering Committee (TSC) or another 3rd party service to maintain a version of the Bedrock Open Source Code.
5. The Bedrock Board of Directors SHOULD require the TSC and/or the Utility Service Provider to automate any prescribed tools that are expected to be used by a node.
6. The Bedrock Board of Directors MUST require the TSC and/or the Utility Service Provider to clearly articulate the mechanism by which a Steward schedules and communicates downtime.

2. General Security Policies

1. A Member MUST maintain and follow IT security policies and practices that are integral to maintaining protection of all services provided in association with the Participation Agreement (“Member Services”). These policies MUST be mandatory for all employees of the Member involved with providing the Member Services. The Member shall designate its CIO or another officer to provide executive oversight for such policies, including formal governance and revision management, employee education, and compliance enforcement.
2. A Member MUST review its IT security policies at least annually and amend such policies as the Member deems reasonable to maintain protection of its Member Services.
3. Because Node administrators are a potential threat vector, a Member MUST maintain and follow its standard mandatory employment verification requirements for all new hires involved with providing its Member Services and will extend such requirements to wholly-owned subsidiaries involved with providing its Member Services. In accordance with the Member's internal process and procedures, these requirements MUST be periodically reviewed and include, but may not be limited to, criminal background checks, proof of identity validation, and additional checks as deemed necessary by the Member. Each Member company is responsible for implementing these requirements in its hiring process as applicable and permitted under local law.

4. Employees of a Member involved with providing its Member Services MUST complete security and privacy education annually and certify each year that they will comply with the Member's ethical business conduct, confidentiality, security, privacy, and data protection policies. Additional policy and process training MUST be provided to persons granted administrative access to components that are specific to their role within the Member's operation and support of its Member Services.
5. If a Member hosts its Node in its own data center, the Member's security policies MUST also adequately address physical security and entry control according to industry best practices.
6. If the Member hosts its Node using a third-party Hosting Provider, the Member MUST ensure that the security, privacy, and data protection policies of the Hosting Provider meet the requirements in this document.
7. A Member MUST make available to the Bedrock Consortium upon request evidence of stated compliance with these policies and any relevant accreditations held by the Member, including certificates, attestations, or reports resulting from accredited third-party audits, such as ISO 27001, SSAE SOC 2, or other industry standards.

3. General Node Policies

A Member Node:

1. MUST be available to run as a Validator Node or Observer Node on any of the formal ledgers associated with the Utility environments (i.e.: prod, stage, dev)
2. MUST run a release of the Bedrock Open Source Code that has been approved and designated by the Bedrock Board of Directors and Technical Steering Committee (TSC).
3. MUST facilitate an upgrade to a new version of the Bedrock Open Source Code within three (3) business days of a new release that has been:
 - a. recommended by the TSC, and
 - b. accepted by the Bedrock Consortium.

4. MUST register all Node configuration data in a timely manner and keep information up to date within three (3) business days of changes.
5. MUST have at least two (2) IT-qualified persons assigned to administer the node, and at least one other person that has adequate access and training to administer the Node in an emergency, such as the network being unable to reach consensus or being under attack. See the TSC regarding specific *Crisis Management Plan* details. See [Issue 23](#).
6. MUST supply contact info for all administrators to the Bedrock Consortium, whose accuracy is tested at least quarterly (e.g., by acknowledging the receipt of an email or text within 24hrs).
7. MUST recover the system from failure in one hour or less.

4. Node Technical Policies

For all ledgers within the Utility environments list, the following requirements apply to Nodes on the `prod` instance of the Utility. These requirements may be downgraded from MUST to SHOULD for any Nodes on ledgers that are for non-production purposes.

1. MUST run on robust server-class hardware.
2. If a Node is run on a VM, the Member:
 - a. MUST run on a mainstream hypervisor that receives timely patches from its vendor or community.
 - b. SHOULD apply hypervisor patches on a regular basis.
3. The Node MUST run in an OS that is dedicated to the validator, i.e., a single-purpose (physical or virtual) machine that MUST run Bedrock Open Source Code, MAY run other software approved by the TSC, and MUST NOT run any other software. Software required to support the node, such as monitoring, backup, and configuration management software, are approved as a general category. However, Members should discuss with the TSC any software packages that transmit between the Member Node and the outside.

4. MUST run a server with compatible versions of the operating systems supported by the Hyperledger Indy Node requirements as documented in the release notes.
5. MUST have adequate compute power (in late 2020, 8 or more cores is considered adequate).
6. MUST have adequate RAM (in late 2020, 32 GB of RAM is considered adequate).
7. MUST have at least 1 TB, with the ability to grow to 2 TB, of reliable (e.g., RAIDed) disk space, with an adequately sized boot partition.
8. MUST have a high-speed connection to the internet with highly available, redundant pipes (as of late 2020, 100 Mbps was considered adequate).
9. MUST have the following dedicated NICs:
 - a. a public NIC for all Validator-to-Validator consensus traffic that is a stable, static, world-routable IP address.
 - b. a private NIC for all CLI-to-Validator traffic
10. MUST prevent traffic originating from the Validator node to reach the Validator's intranet domain.
11. MUST be implemented in a way that does not endanger Bedrock's high availability architecture, which is pool-based rather than node-based. Nodes should not take more responsibility for high availability than what is contemplated by the Node Selection Algorithm. For example, they should listen at exactly one pair of network addresses (see 3.9 above), using exactly one set of keys to respond to BBU/Indy protocol traffic at any one time, and adhere to a minimal failover recovery delay period specified by the Bedrock Consortium (or 30 seconds if not specified).
12. MUST have a system clock that is demonstrably in sync with well-known NTP servers.
13. SHOULD have a power supply consistent with high availability systems.

5. Node Security Policies

A Member:

1. MUST maintain its [CLI Private Key](#) on a separate machine from the machine that runs their node. This machine, called the “CLI (Command Line Interface) system”, uses the *CLI Private Key* to authorize the Node to participate in the pool, and is thus the basis for trust for the node and the Member's identity on the network. The CLI system is not required to have high-end hardware, but in terms of IT best practices for security, it must meet or exceed the standards for the Node (see following items).
2. MUST provide certification that their Node runs in a locked datacenter with appropriate levels of security, including the specifications that they target (e.g., SSAE 16 type II compliance; other standards may also be acceptable).
3. MUST assert that their Node is isolated from internal systems of a Member (because the Validator Node is publicly visible and thus an inappropriate candidate for access to privileged internal networks).
4. MUST assert that their Node, and its underlying systems, uses state-of-the-art authentication for remote access via SSH with key plus password plus source IP firewall rule.
5. SHOULD implement two-factor authentication for SSH access.
6. MUST NOT allow access (remote or local) to the Node or CLI systems by anyone other than assigned admins.
7. MUST apply the latest security patches within one (1) week or less (24 hours or less is recommended).
8. MUST attest that the Node runs on a server protected by a firewall that, at minimum:
 - a. Disallows public ingress except on ports used by the Node software (different machines may choose to expose ledger features on different ports, so no standard port setup is required).
 - b. Optionally enables SSH, Remote Desktop, and similar remote access tools but constrains ingress for these tools in some way that excludes the public but allows access for admins.

- c. Locks down egress ports to limit the ability to jump from Node to some other location.
- 9. MUST run a set of TSC prescribed tools and receive TSC approval of the results before the Node is authorized to participate in consensus.
- 10. MUST run a set of TSC prescribed tools from time to time as requested by the TSC and provide the test results report to the TSC within three (3) business days.

See [Issue 24](#).

6. Node Operating Policies

A Member:

- 1. MUST equip at least two (2) technical points of contact responsible for administering the Member Node with an SMS-capable device for alerting.
- 2. SHOULD aim to achieve at least 99.9% (three nines) uptime for their Node (this amounts to about 1.4 minutes of downtime per day or 9 hours per year).
- 3. SHOULD coordinate downtime with other Members in advance via a mechanism as determined from time to time by agreement between the TSC and any other relevant Bedrock Consortium Governing Body.

7. Node Selection Algorithm

- 1. The TSC will take direction from the Bedrock Consortium Board of Directors, or a designated Bedrock Workgroup, regarding the configuration parameters associated with the deployment of the Node Selection Algorithm.
- 2. The selection of active Validator Nodes at any point in time, at least on the BBU, MUST be governed by the Node Selection Algorithm.
- 3. Non-technical inputs or policy decisions implemented by the Node Selection Algorithm MUST be approved by the Bedrock Consortium Board of Directors.
- 4. At any point in time, the Node Selection Algorithm MUST represent the TSC's best efforts at designing an algorithm that applies the Core Principles of the

Bedrock Consortium Governance Framework. Recognizing the inherent tension and tradeoffs between some of the Core Principles, the design of this algorithm should give priority to balancing:

- a. The Decentralization by Design principles, in particular the principles of Diffuse Trust and High Availability. See *Diversity Goals* below.
 - b. The Security by Design principles, in particular the principles of System Diversity and Secure Failure. See *Diversity Goals* below.
5. A human-readable, understandable, and explainable description of the current design of the algorithm as approved by the TSC MUST be published by the TSC in the official Sovrin Foundation Code Repository and made visible to all Members via a web page on the Bedrock Consortium website.

8. Reporting Policies

1. A Member MUST report to the responsible Bedrock Consortium Governing Body any substantive change to the configuration or location of a Node within five (5) business days of the change.

9. Diversity Goals

While the *Node Selection Algorithm* will be tuned from time-to-time to address Performance as well as Decentralization Security by Design principles, the following diversity guidelines SHOULD be considered:

Concern	Policy
Should restrictions be applied that limit the number of nodes in the active Validator Pool that are hosted in a specific data center?	See IaaS Policy
Should restrictions be applied that limit the number of nodes in the active Validator Pool that are hosted in a specific geolocation?	See IaaS Policy
Should restrictions be applied that limit the number of nodes in the active Validator Pool that can be hosted on the same IaaS?	YES - See IaaS Policy
Should restrictions be applied that limit the number of nodes in the active Validator Pool that can be hosted by the same hosting provider?	NO - See Hosting Provider Policy

IaaS Policy

1. If a Steward desires to take on the compliance costs for in-house hosting certification, this will add diversity to the Utility.
2. Some Stewards MAY desire to meet the needs of their membership obligations using external cloud providers that offer the necessary security and compliance certifications and offers world-wide data center coverage. The following SHOULD be considered when Stewards leverage any form of outsourced cloud computing (*Infrastructure as a service (IaaS)*, *Software as a service (SaaS)*, or *Platform as a service (PaaS)*):
 - a. In 2019, [Gartner listed](#) the following top 6 global enterprise cloud providers: AWS, Microsoft, Alibaba, Google, Oracle and IBM. These providers have the ability to meet two key requirements for Stewards:
 - i. Standards compliance and certification;
 - ii. Many (>15) availability zones across numerous (>5) geographic regions.
 - b. There is no simple way to determine the appropriate degree of granularity relative to geolocation restrictions. Instead, limits SHOULD be

applied to the number of nodes across availability zones within a particular IaaS.

- i. No more than 10% of total Active Validator Pool SHOULD be hosted in the same availability zones of an IaaS.
- ii. Assuming an Active Validator Pool of 25, this would be no more than 2 nodes on any given availability zone for an IaaS.
- c. To minimize the impact IaaS vulnerabilities may have on consensus, no more than 33% of the Active Validator Pool should be running on a specific IaaS.
- d. Assuming an Active Validator Pool of 25, this would imply that no more than 8 nodes should be hosted on any one IaaS.

Hosting Provider Policy

The relationship between a Steward and a Hosting Provider is outside the scope of the BBU-GF. Hosting provider decisions have financial impacts on Stewards and as a result the Consortium SHOULD NOT insert itself into that decision making process.

While no restrictions are suggested, a Steward SHOULD expect hosting providers to offer multi-cloud hosting options for Indy-Node SaaS services so that IaaS policies can be observed across the BBU.

Endorser Business Policies

Transaction Endorser Business Policies

This is a Controlled Document of the Bedrock Governance Framework was approved by the Bedrock Consortium Board of Directors.

Document Name	Transaction Endorser Business Policies
Version	v0.9
Approval Date	
Status	Pre-Launch Phase: Governance Framework Development
Governs	Operational Requirements, Contractual Obligations, Author Vetting
Governed By	Bedrock Governance Framework Work Group, Sovrin Technical Steering Committee

General

All members that are approved to be *Transaction Endorsers* must adhere to the procedures and policies outlined herein.

Operational Requirements

1. They are **obligated to use Consortium approved endorser software and accountable for vetting the entities** (*Transaction Authors*), that submit write requests.
2. MUST perform entitlement checks with the ledger a prior of endorsing write transactions.

Contractual Obligations

All members approved for the role of *transaction Endorser* MUST: * Sign Transaction Endorser Agreement * Sign Transaction Endorser DPA Agreement

Transaction Author Vetting

1. Ensure the Transaction Author has signed the Bedrock Consortium Transaction Author Agreement

Endorser Technical and Organizational Policies

Endorser Technical and Organizational Policies

This is a Controlled Document of the Bedrock Governance Framework was approved by the Bedrock Consortium Board of Directors.

Document Name	Endorser Technical and Organizational Policies
Version	v0.9
Approval Date	
Status	Pre-Launch Phase: Governance Framework Development
Governs	General Security Policies, Node Technical Policies, General Security Policies, Node Security Policies, Operating Policies, Node Selection Algorithm, Permissioned Test Network Policies, Reporting Policies
Governed By	Bedrock Governance Framework Work Group, Sovrin Technical Steering Committee

1. General Security Policies

1. Transaction Endorser MUST maintain and follow IT security policies and practices that are integral to maintain protection of all services provided in association with the Transaction Endorser Agreement ("Endorser Services"). These policies MUST be mandatory for all employees of the Endorser involved with providing the Endorser Services. The Transaction Endorser shall designate its CIO or another officer to provide executive oversight for

such policies, including formal governance and revision management, employee education, and compliance enforcement.

2. Transaction Endorser MUST review its IT security policies at least annually and amend such policies as the Endorser deems reasonable to maintain protection of its Endorser Services.
3. Transaction Endorser MUST maintain and follow its standard mandatory employment verification requirements for all new hires involved with providing its Endorser Services and will extend such requirements to wholly-owned subsidiaries involved with providing its Endorser Services. In accordance with the Transaction Endorser's internal process and procedures, these requirements MUST be periodically reviewed and MUST include, but may not be limited to criminal background checks, proof of identity validation, and additional checks as deemed necessary by the Transaction Endorser. Each Transaction Endorser company is responsible for implementing these requirements in its hiring process as applicable and permitted under local law.
4. Employees of a Transaction Endorser involved with its Endorser Services MUST complete security and privacy education annually and certify each year that they will comply with the Transaction Endorser's ethical business conduct, confidentiality, security, privacy, and data protection policies. Additional policy and process training MUST be provided to persons granted administrative access to components that are specific to their role within the Transaction Endorser's operation and support of its Endorser Services.
5. If a Transaction Endorser performs its Endorser Services in its own data center, the Transaction Endorser's security policies MUST also adequately address physical security and entry control according to industry best practices.
6. If a Transaction Endorser performs its Endorser Services using a third-party Hosting Provider, the Transaction Endorser MUST ensure that the security, privacy, and data protection policies of the Hosting Provider meet the requirements in this document.
7. Transaction Endorser MUST make available to the Bedrock Consortium upon request evidence of stated compliance with these policies and any relevant accreditations held by the Transaction Endorser, including certificates,

attestations, or reports resulting from accredited third-party audits, such as ISO 27001, SSAE SOC 2, or other industry standards.

2. Security Incident Policies

1. Transaction Endorser MUST maintain and follow documented incident response policies consistent with NIST guidelines for computer security incident handling and will comply with data breach notification terms of the Transaction Endorser Agreement.
2. Transaction Endorser MUST investigate unauthorized access of which the Transaction Endorser becomes aware (security incident), and the Transaction Endorser will define and execute an appropriate response plan. The Bedrock Consortium may notify the Transaction Endorser of a suspected vulnerability or incident by submitting a technical support request.
3. Transaction Endorser MUST notify the Bedrock Consortium without undue delay upon confirmation of a security incident that is known or reasonably suspected by the Transaction Endorser to affect the Consortium. The Transaction Endorser will provide the Bedrock Consortium with the reasonably requested information about such security incident and the status of any of the Transaction Endorser remediation and restoration activities.

3. General Technical Policies

In performing its Endorser Services, Transaction Endorser MUST:

1. Comply with all relevant Bedrock Consortium Ledger Access Policies.
2. Follow any additional guidelines published by the Technical Steering Committee on the Bedrock Consortium website or github site.

© 2020 by Bedrock Consortium. This work is licensed under the Creative Commons Attribution-ShareAlike 4.0 International License (<http://creativecommons.org/licenses/by-sa/4.0/>).

Economic Policies

Economic Policies

This is a Controlled Document of the Bedrock Governance Framework was approved by the Bedrock Consortium Board of Directors.

Document Name	Economic Policies
Version	v0.9
Approval Date	
Status	Pre-Launch Phase: Governance Framework Development
Governs	Membership, Incentives, Regulatory Compliance
Governed By	Bedrock Governance Framework Work Group

Membership

The Bedrock Consortium MUST establish economic procedures that will achieve the following:

1. Procurement

- a. Collection of membership dues.
- b. Sale and renewal of Subscription plans.
- c. Membership management and ledger transaction usage that track membership entitlements and status. See [Membership Management System](#).

2. Currency

- a. All income MUST be denominated in U.S. Dollars (USD).

3. Publication

- a. All Bedrock Consortium subscription plan offerings SHOULD be publicly disclosed on the Bedrock Consortium website.
- b. The Bedrock Consortium SHOULD publish the current schedule of Membership Fees on the Bedrock Consortium website.

Utility Service Providers

The Bedrock Consortium MUST establish economic procedures that will achieve the following:

1. Bidding Process
2. Request for Proposal publication process.
3. Provider selection process.
4. Procurement
5. Payment process from Directed Fund for service providers.

Incentives

The Bedrock Consortium MAY provision economic incentives designed to for the following purposes:

1. To reward Developers, Agencies, or other community members to contribute to the Bedrock Open Source Code or to any other community asset of benefit to the Consortium, the Bedrock Business Utility or organizations such as the ToIP Foundation.

Regulatory Compliance

The Bedrock Consortium MUST provide auditable information (IFRS, International Financial Reporting Standards) about all monetary collections and disbursements. **NEED TO VALIDATE**

Certification Mark Policies

Trust Marks

1. The Consortium MAY publish the set of Trust Marks designated in this document on the BBU website together with:
 - a. A link to these policies governing their usage.
 - b. The Trust Mark License.
 - c. Instructions for publishing a Self-Certification Page.

Stewards

1. Stewards who are active members in good standing:
 - a. Any Steward that was a member upon the launch of the Utility MAY use the Trust Mark designated for Founding Stewards under the terms of the Steward Agreement.
 - b. MAY use the Trust Mark designated for Stewards under the terms of the Steward Agreement.

Agencies

1. Agencies who meet the requirements of Self-Certification according as defined in the Trust Assurance Framework and who wish to signal that conformance publicly MUST do so by:
 - a. Using the Trust Mark designated for Self-Certified Agencies under the terms of the Trust Mark License.
 - b. Publishing a Self-Certification Page.

Developers

1. Developers who meet the requirements of Self-Certification as defined in the Trust Assurance Framework and who wish to signal that conformance publicly MUST do so by:
 - a. Using the Trust Mark designated for Self-Certified Developers under the terms of the Trust Mark License.
 - b. Publishing a Self-Certification Page.

Directory

1. The Consortium MAY offer a public directory of Agencies, Developers, or other Infrastructure Roles who meet the requirements of this Controlled Document.
2. Participation in such a public directory MUST be opt-in.
3. All listings in such a public directory that are based on Self-Certification MUST include a link to the Self-Certification Page.

Trusted Network Policies

Ecosystem of Trust

This is a Controlled Document of the Bedrock Governance Framework was approved by the Bedrock Consortium Board of Directors.

Document Name	Trusted Network Policies
Version	v0.9
Approval Date	
Status	Pre-Launch Phase: Governance Framework Development
Governs	General Trust Policies
Governed By	Bedrock Governance Framework Work Group

Network Trust Perspective

The Bedrock Consortium strives to establish and position ledgers, such as the Bedrock Business Utility, to be reliable and trusted ledgers for businesses seeking to perform decentralized identifier verification tasks. However, each entity operating in the roles of issuer or verifier MUST arrive at their own independent determination of a trusted identity network.

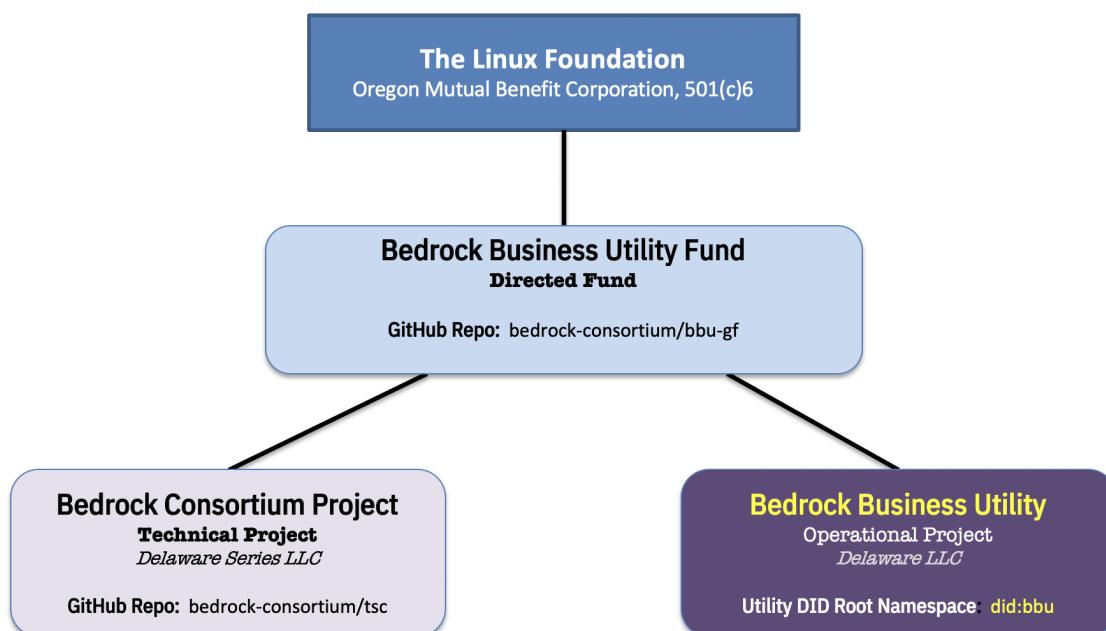
General Trust Policies

The Governing Board for the Bedrock Consortium WILL work with the ToIP Ecosystem Foundry Working Group to help position the Bedrock Business Utility as a trusted utility for use by ecosystem projects.

Architecture

Introduction

The Bedrock Business Utility (the "Utility") is governed by the Bedrock Consortium as a dedicated public-permissioned blockchain ledger. The nodes of this immutable Utility are hosted by a variety of business entities around the world, called Stewards. The Utility is intended to enable Transaction Authors (see below) to publish decentralized identifiers (DIDs) and other cryptographic data structures required for the issuance and verification of digital credentials.



The Utility is legally represented as three (3) distinct but related legal entities which are associated with a collection of contractual instruments. The *Bedrock Business Utility Fund* (the “Directed Fund”), is a directed fund project of The Linux Foundation (the “LF”). The Directed Fund serves two purposes:

1. Manage the operation and maintenance of the Bedrock Business Utility (“the Utility”), a LF Operational Project (a Delaware series limited liability company)
2. Support for the Bedrock Consortium Project, (the “Technical Project”), an open source project, a LF Network Project.

It is expected that the Utility will be used primarily by businesses who have a need to exchange trusted data such as digital credentials. The credentials themselves are never written to the Utility so issuers of these credentials (*Transaction Authors*) have no need to write data to the Utility. This approach avoids issuers increasing risks associated with personal data under data protection regulations such as the EU General Data Protection Regulation (GDPR), the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA), or the California Consumer Privacy Act (CCPA).

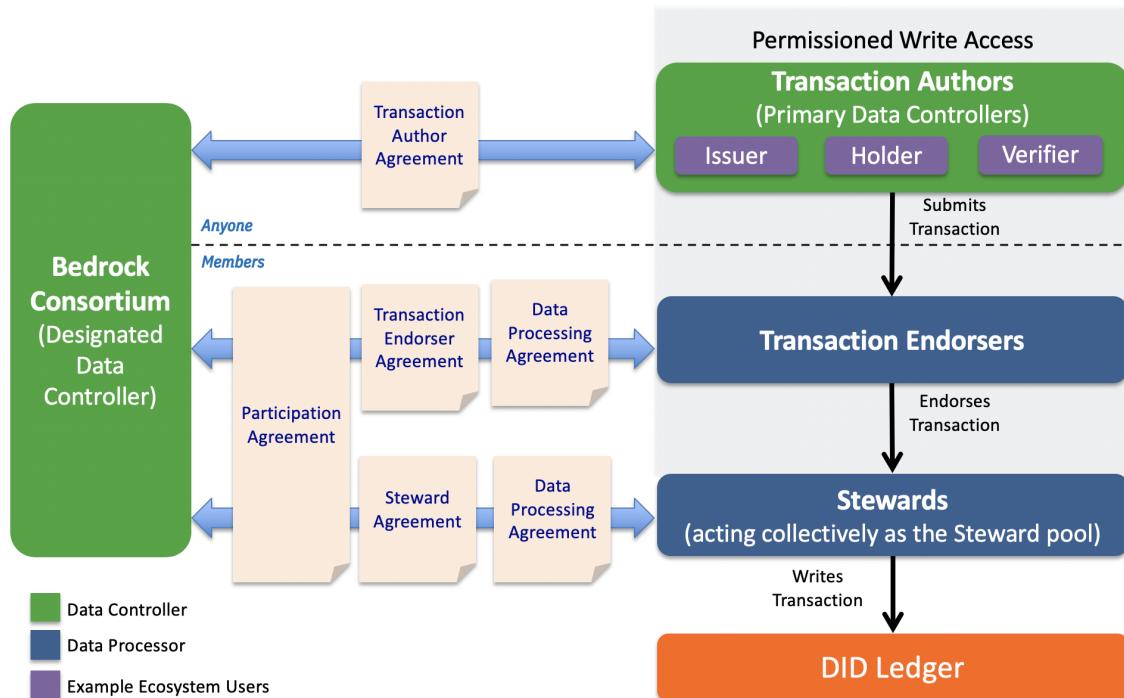
Data Protection

The Sovrin Foundation in conjunction with its legal counsel [Perkins Coie](#) published a white paper providing a detailed legal analysis of the applicability of the GDPR to the Sovrin Utility and Sovrin Network. The [GDPR Position Paper](#) assesses data protection requirements at Layers 1-3 of the ToIP Stack.

The Bedrock Consortium recognizes this work-product as prior art given its applicability to any public identity utility. This paper is a foundational legal document for the importance of permissioned-write access to the ledger. See [Issue 16](#) pertaining to the storage location of this paper after the transition effort of the Sovrin Foundation.

Legal Architecture

The following figure is a visual illustration of the key roles and agreements in the Bedrock Consortium's legal framework for regulatory compliance with data protection laws. Although it uses terms from the GDPR, it is intended for compliance with general data protection regulations.



The following sections explain the actors, roles, policies, and legal agreements depicted in this diagram. Note that formal definitions for all terms that appear in First Letter Capitals are provided in the [Glossary](#).

Actors & Roles

Bedrock Consortium

The Bedrock Consortium is an international non-profit public trust organization chartered to provide governance for the Bedrock Business Utility. Represented by the Governing Board of the Utility, the Consortium represents the *Designated Data Controller*. In this role, the Consortium is a broker between Transaction Authors, the *Primary Data Controller*, and other Utility actors.

Consortium Members

In order to participate in the Consortium as either a Steward, a Transaction Endorser or both; the desired participant MUST sign the Participation Agreement. This agreement allocates write access entitlements by membership level.

Transaction Authors

A Transaction Author is any Organization who submits a Transaction to be written to the Utility. This role in the BBU-GF is available to both members and non-members. As explained below, under the Permissioned Write Access policies of the BBU-GF, only Organizations may write Transactions. Transaction Authors may write any data type supported by the Utility – see [What Goes On The Ledger?](#)

Transaction Endorsers

A Transaction Endorser is an Organization that has been approved by the Bedrock Consortium to endorse Transactions on behalf of Transaction Authors. The role of Transaction Endorser is specified by the Permissioned Write Access policies of the BBU-GF. Transaction Endorsers add their digital signature to a Transaction so it will be accepted and written by the Stewards. Transaction Endorsers MUST enter into both the Transaction Endorser Agreement and the Transaction Endorser Data Processing Agreement with the Bedrock Consortium.

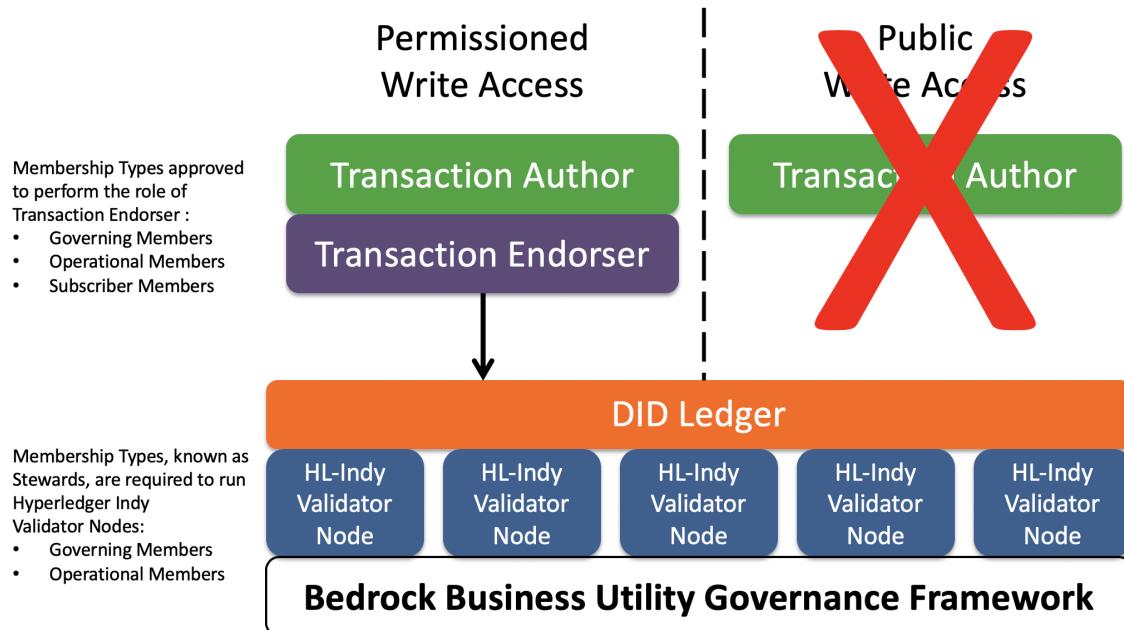
Subscribers

Subscribers are trusted institutions who desire to participate in the Consortium as Transaction Endorsers. This membership level allows desiring participants to procure a limited number of write transaction units on an annual basis.

Stewards

Stewards are trusted institutions who operate a Node of the Utility. Stewards MUST meet the qualifications specified in [Member Business Policies](#) and [Member Technical and Organizational Policies](#). Stewards must enter into both the Steward Agreement and the Steward Data Processing Agreement with the Bedrock Consortium. Stewards are automatically qualified to be Transaction Endorsers but they MUST sign the appropriate Transaction Endorser contracts with the Bedrock Consortium.

Utility Access Policies



Permissioned Write Access

This is the set of policies that require Transaction Authors to obtain the endorsement of a Transaction Endorser in order to write a Transaction to the Utility. There are two primary reasons for the Permissioned Write Access policy:

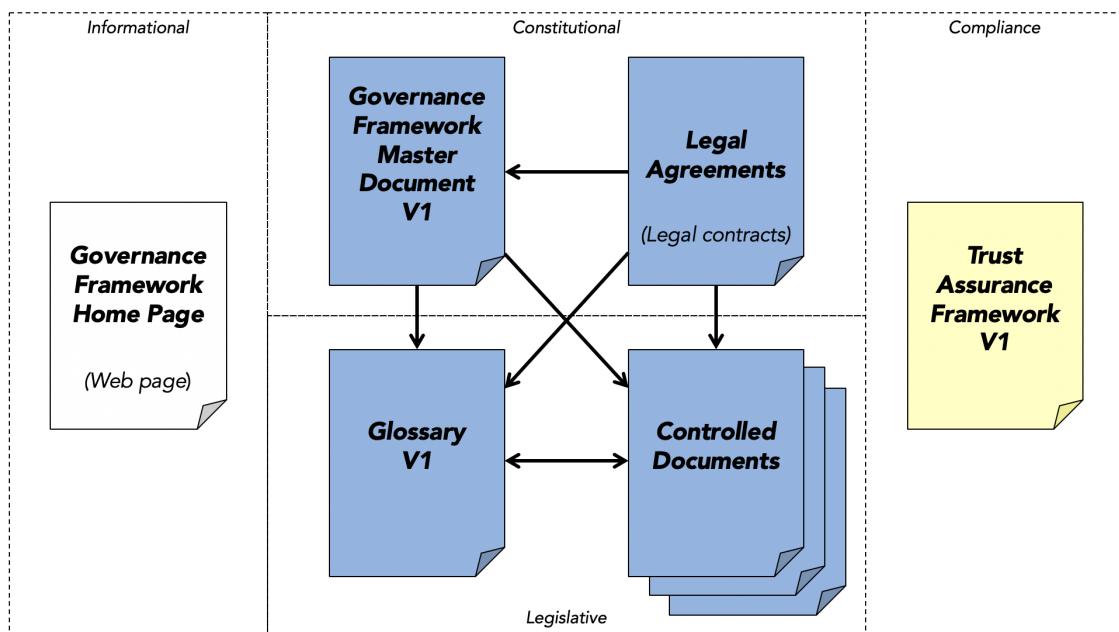
1. It protects the Utility by requiring Transaction Endorsers, who have a direct contractual relationship with the Bedrock Consortium to enforce the Permissioned Write Access policies, to ensure that a Transaction Author Agreement is in effect and to leverage an allocated write unit as a form of payment for a Transaction. Write Units are acquired based on Membership Type.
2. It reduces the risk of Personal Data being written to the Utility as that is currently prohibited under the Permissioned Write Access policies. The Bedrock Consortium feels this protection is necessary under the current regulatory uncertainty regarding Personal Data on an immutable public ledger. See the *Data Protection* section of this document for more details.

Public Write Access

Under Public Write Access policies, the requirement of a Transaction Endorser signing a Transaction Authors request is eliminated; anyone would be able to write to the Utility by following a programmatic process that aims to provide the necessary assurances against privacy compliance risks. **This form of access to the Utility is prohibited under the BBU-GF.**

Legal Document Architecture

Primary Legal Agreements



Participation Agreement

This is the contractual agreement between the Bedrock Consortium and all members. It has been developed by the Linux Foundation in support of Directed Fund projects. This agreement is the binding agreement for all members.

Transaction Author Agreement

This is the contractual agreement between the Bedrock Consortium and all Transaction Authors. It has been developed specifically to protect the right of every Transaction Author to have and hold self-sovereign identity credentials

while also protecting the Utility and the infrastructure provided by the Bedrock Consortium as a global public utility. It is intended to give effect to the data protection rights of all Transaction Authors while recognizing the technical and security requirements of a public-permissioned immutable Utility. As part of the Transaction Author Agreement, every Transaction Author also agrees to be bound by the terms and conditions applicable to the Transaction Author as a controller under the Steward Data Processing Agreement and the Transaction and the Transaction Endorser Agreement to include a Data Processing Agreement. The Utility itself is the authoritative record of all Transaction Author Agreement signatures.

Transaction Endorser Agreement

This is the contractual agreement between the Bedrock Consortium and all Transaction Endorsers. This agreement is simpler in scope than the Transaction Author Agreement. It is limited to enforcing Permissioned Write Access policies and verifying that Transaction Authors have executed the Transaction Author Agreement. The Transaction Endorser Agreement requires that the Transaction Endorser separately execute the Transaction Endorser Data Processing Agreement and includes a current version of the Transaction Author Agreement as an Appendix. This agreement **does not** address the exchange of payment (value) between the Transaction Endorser and the Transaction Author. Such usage fees associated with the allocation of write transaction entitlements is *out-of-scope* for the BBU-GF.

Steward Agreement

This is the contractual agreement between the Bedrock Consortium and all Stewards. It covers all the rights and obligations of the Bedrock Consortium and Stewards under the Bedrock Governance Framework. The Steward Agreement requires that the Steward separately execute the Steward Data Processing Agreement.

Data Processing Agreements (DPAs)

Transaction Endorser DPA

This is the DPA required of all Transaction Endorsers acting as Data Processors for the Transaction Author as primary Data Controller and the Bedrock Consortium acting as the Designated Data Controller. It requires that the Transaction Endorser implement its own set of Technical and Operational Measures (TOMs) that MUST meet or exceed the Transaction Endorser Technical and Organizational Policies (TOPs) specified in the Bedrock Governance Framework.

Steward DPA

This is the DPA required of Stewards. It requires that the Steward implement its own TOMs that meets or exceeds the Steward TOPs.

Technical and Organizational Policies (TOPs)

Transaction Endorser TOPs

This is the set of policies in the Bedrock Governance Framework that establish the minimum technical and organization policies and procedures that a Transaction Endorser MUST implement in its own Technical and Operational Measures (TOMs) to provide adequate security, privacy, and data protection for Transaction Authors and the Bedrock Consortium.

Steward TOPs

Similar to the Transaction Endorser TOPs, this is the set of policies in the Bedrock Governance Framework that establish the minimum technical and organization policies and procedures that a Steward must implement in its own Technical and Operational Measures (TOMs) to provide adequate security, privacy, and data protection for Transaction Authors and the Bedrock Consortium.

Member Agreements

Members are required to enter into contractual agreements with the Bedrock Consortium.

All Participants

All members MUST sign the [Participation Agreement \(MS-WORD\)](#)

Stewards

Any member that is required by the Participation Agreement to [host a utility infrastructure node](#) is considered a Steward and MUST sign these contractual instruments:

- [Steward Agreement \(MS-WORD\)](#)
- [Steward Data Processing Agreement \(MS-WORD\)](#)
- [Transaction Endorser Agreement \(MS-WORD\)](#)
- [Transaction Endorser Data Processing Agreement \(MS-WORD\)](#)
- [*Optional* Transaction Author Agreement \(MS-WORD\)](#)

Subscribers

- [Transaction Endorser Agreement \(MS-WORD\)](#)
- [Transaction Endorser Data Processing Agreement \(MS-WORD\)](#)
- [*Optional* Transaction Author Agreement \(MS-WORD\)](#)

Non-Member Agreements

Any non-members that desires to use the Utility MUST enter into certain contractual agreements between the Bedrock Consortium.

Transaction Authors

- [Transaction Author Agreement \(MS-WORD\)](#)

Trust Assurance

Bedrock Trust Assurance Framework

Introduction

The Bedrock Business Utility ("BBU") is intended to provide supporting infrastructure to maintain a sustainable permissioned identity utility that is structured as an enterprise safe-space and purpose built for trusted commerce.

Users of the BBU, namely Issuers and Verifiers of digital credentials, expect a level of assurance pertaining to the reliability and integrity of the ledger. Those users who are members of the Bedrock Consortium have a vested interest understanding the level of assurance that can be assigned to the BBU. Those users who seek public read-only access for verification purposes also desire an understanding the level of assurance to help set business verification policies but they do not have a stake in the n

Assurance Requirements

The BBU aspires to ensure reliability, low processing latency, and a maximum uptime of the service. The Level of Assurance that can be asserted by the BBU Governance Framework will evolve over time depending on a number of factors including:

- Member Compliance
 - Adherence to technical and operating policies operating policies
 - Contract status
- Ledger Reliability
 - Probability that verification requests (ledger reads) will operate without failure for a specified number of transactions or for a specified period of time and within an acceptable response-time.

- Probability that transaction author requests (ledger writes) will operate without failure for a specified number of transactions or for a specified period of time and within an acceptable response-time.
- Ecosystem Trust Factor

As the BBU matures towards a production ready and actively used ledger, the degree of assurance measures that will be in place will vary.

Pre-Production Phase

1. No assurances for public use (read transactions).
2. Membership status will be public through Bedrock Consortium website.

Early Production Phase

1. No assurances for public use (read transactions).
2. Membership status will be public through Bedrock Consortium website.
3. Ledger Reliability expectations will be set and audit procedures will be established.

General Production

1. No assurances for public use (read transactions).
2. Membership status will be public through Bedrock Consortium website.
3. Ledger Reliability expectations will be set and audit procedures will be established.

Versioning

Each version of this document is tied to the BBU Governance Framework at a specific point of time.

Terminology

All terms in First Letter Capitals that are not defined in this document (as called out in a specific section) are defined in the [Glossary](#).

Purpose

The purpose of the BBU Trust AssuranceFramework is to identify:

1. The Trust Elements that Trust Actors assert in relationship to the BBU.
2. The The BBU Roles that assert and rely upon trust.
3. Generally-Accepted, Bedrock-Specific, or Domain-Specific Trust Criteria used in the evaluation of trust associated with the BBU.
4. The Trust Assertions that BBU Roles make against Trust Criteria.
5. The Trust Evidence that Trust Actors produce to create assurance regarding their trust assertions.
6. The Trust Mechanisms in place to assert and evaluate trust.
7. The process of Trust Governance whereby trust assertions are evaluated and deemed trustworthy, so they can be relied upon by Relying Parties (BBU Consumers).

Level of Assurance

This document describes the Level of Assurance a Relying Party can derive from the BBU Governance Framework. This section defines the maximum level.

The BBU Governance Framework claims a **maximum** level of a **reasonable** Level of Assurance.

In May 2013, the Committee of Sponsoring Organizations of the Treadway Commission (COSO)updated its [Internal Control—Integrated Framework](#) (the original framework). The original framework has gained broad acceptance and is widely used around the world. It is recognized as a leading framework for designing, implementing, and conducting internal control and assessing the effectiveness of internal control. Internal control is defined as follows:

Internal control is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.

This definition reflects certain fundamental concepts. Internal control is:

- Geared to the achievement of objectives in one or more categories—operations, reporting, and compliance
- A process consisting of ongoing tasks and activities—a means to an end, not an end in itself
- Effected by people—not merely about policy and procedure manuals, systems, and forms, but about people and the actions they take at every level of an organization to affect internal control
- Able to provide reasonable assurance—but not absolute assurance, to an entity's senior management and board of directors
- Adaptable to the entity structure—flexible in application for the entire entity or for a particular subsidiary, division, operating unit, or business process This definition is intentionally broad. It captures important concepts fundamental to how organizations design, implement, and conduct internal control, providing a basis for application across organizations that operate in different entity structures, industries, and geographic regions.

The [ICAEW definition of a reasonable assurance audit engagement](#) is: Where the practitioner needs to reduce the assurance engagement risk (the risk that an inappropriate conclusion is expressed when the information on the subject matter is materially misstated) to an acceptably low level as the basis for a positive form of expression of the practitioner's conclusion. Such risk is never reduced to nil and therefore, there can never be absolute assurance. Per the ICAEW guidance on management of risk and liability , relying parties may perceive less than reasonable assurance based on their evaluation of the BBU Governance Framework and the BBU Trust AssuranceFramework but not more.

Trust Elements

The following Trust Elements guide the development of specific Trust Criteria asserted by Trust Actors in the BBU. These are based on the AICPA Trust Services Criteria based on COSO Internal Control - Integrated Framework, for use in attestation or consulting engagements to evaluate and report on controls over information and systems (a) across an entire entity; (b) at a subsidiary, division,

or operating unit level; (c) within a function relevant to the entity's operational, reporting, or compliance objectives; or (d) for a particular type of information used by the entity.

- Security. Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.
- Availability. Information and systems are available for operation and used to meet the entity's objectives.
- Processing integrity . System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.
- Confidentiality. Information designated as confidential is protected to meet the entity's objectives.
- Privacy. Personal information is collected, used, retained, disclosed, and disposed to meet the entity's objectives.

BBU Roles Making Trust Assertions

The following BBU Roles make Trust Assertions with regard to the Trust Elements to Relying Parties within the Bedrock Community:

1. Bedrock Consortium (including the Governing Board).
2. Steward.

Trust Criteria

Bedrock-Specific Trust Criteria

For the BBU Governance Framework, the only Trust Criteria in operation are self-developed by the Bedrock Consortium and appear in section 10 and in an Addendum to that document. It comprises governance Policies the Bedrock Consortium has set for itself and the [Bedrock Member Business Policies](#) and [Bedrock Member Technical Policies](#) it mandates for Stewards.

Trust Evidence

Trust assertions are empty without evidence to support it. The following are examples of Trust Evidence that are used to support Trust Assertions for the BBU Governance Framework.

1. Signed Contracts.
2. Signed Agreements.
3. Configurations.
4. Signed Approvals.
5. Policies.
6. Procedures.
7. Logs.
 - a. Security.
 - b. Application.
 - c. System.
 - d. Database.

Incident Records

For the BBU Governance Framework, see the Trust Assurance Matrix (Addendum) for the specific Trust Evidence used in this version of the BBU Trust AssuranceFramework.

Trust Actors

The following is the set of Sovrin Entities who play a role in the Sovrin Governance Framework in assessing and opining on Trust Assertions in the Sovrin Network.

1. Bedrock Governing Board. Issues the Policies within the Sovrin Governance Framework and has the right to approve and suspend Stewards from the Sovrin Network. It has the right to perform Self-Certification to evoke assurance from Relying Parties.
2. Stewards. Agree to the Steward Agreement and perform Self-Certification of compliance with the Steward Business Policies and Steward Technical Policies.

3. Legal Authorities. Enforce laws in the Jurisdictions of the Bedrock Consortium and Stewards and mediates the Sovrin Steward Agreement if challenged.

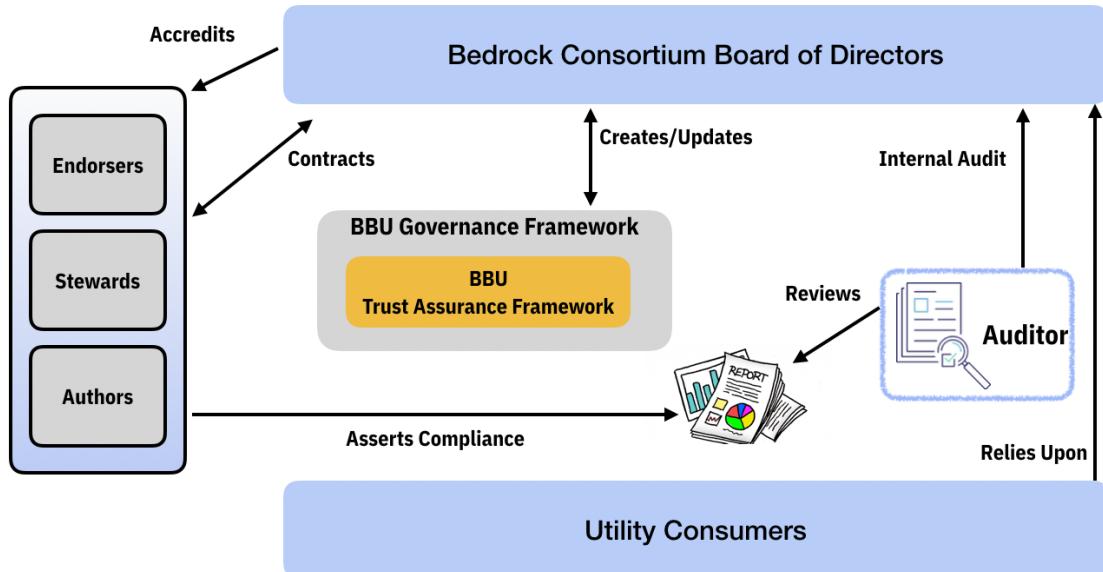
Trust Mechanisms

The following are actions that the Bedrock Consortium takes to assert and assure trust:

1. Contracts and Agreements
2. Self-Assertion a. Bedrock Consortium Trust Criteria Compliance b. Legal Compliance

Trust Governance

The following is a graphical and procedural depiction on how trust asserted from BBU Roles are currently received, assessed, and relied upon in the BBU.



For the BBU Governance Framework:

1. The Bedrock Governing Board has established the BBU Governance Framework and this BBU Trust Assurance Framework. It has created its own Policies and those it requires of Stewards in their Role within the BBU.

2. The Bedrock Governing Board requires members to sign the contractual instruments and perform Self-Certification that the member is compliant with the [Bedrock Member Business Policies](#) and [Bedrock Member Technical Policies](#). This Self-Certification is reviewed by the responsible Bedrock Governing Body and reported to the Bedrock Governing Board prior to approval of the Steward.

Trust Assurance Matrix

The BBU Trust Assurance Matrix is a tabbed spreadsheet which correlates existing Bedrock Governance Framework Policy statements across BBU Governance Framework documents and relevant stakeholders. This matrix is the foundation of self and third-party audits needed to verify compliance to the Sovrin Governance Framework.

© 2020 by Bedrock Consortium. This work is licensed under Creative Commons Attribution-ShareAlike 4.0 International License (<http://creativecommons.org/licenses/by-sa/4.0/>).

FAQ

What is a financially incentive for a Steward to continue long-term participation?

Each participating member will need to make an annual decision on the ROI of their investment.

It is assumed that some members will charge their clients for access to their entitlement transactions while others may not charge and include such access as a perk/benefit.

Frequently asked question?

Answer

Frequently asked question?

Answer

Contact us

Bedrock Business Consortium

Contact Board of Directors

Email bod@bbu.sovrin.org

NOTE: Need to setup emails and or Google Groups/Forums

Contact Governance Framework Working Group

Email bbugf-wg@bbu.sovrin.org

Contact Identity Utility Administrator

The Sovrin Foundation is the provider of administrative services to the Bedrock Business Consortium. Our Network Administrator is:

Name	Email	Phone
xxxxx	sovadmin@bbu.sovrin.org	999-999-9999