Intended Audience

This document is intended for users of the Jiritsu Ledger dApp. Typically this will be Proof Providers, Tokenizers, Marketplaces and Blockchians.

Overview:

In the Jiritsu system, a token or contract issuers claims proof on the Jiritsu L1 blockchain via a Jiritsu dApp. The process involves engaging with a data provider to obtain proof data with exclusive access via an access key. By providing the contract ID and blockchain name into the dApp, the contract is verified. By doing so the contract is immutably bonded with the proof data on the Jiritsu contract. The contract ID and blockchain name serve as unique identifiers for the contract. The system supports any blockchain, requiring only that the dApp can look up and verify the contract's existence.

Summary of system flow:

In the system, a token or contract issuer claims a proof on the Jiritsu L1 blockchain by interacting with a Jiritsu dApp. The process involves the following steps:

1. Obtaining the proof data:
    a. Engagement with Data Provider: The user agrees with the proof provider who has generated the proof and written it to the L1. This agreement may involve payment or another form of consent.

    b. Access Key Permission: Upon agreement, the user receives a key that grants permission to access the data.

2. Providing Token or Contract information
    a. Entering Blockchain Information: The user then enters the blockchain name and the contract ID on the dApp. The dApp supports any and all blockchains and integration with a blockchain, the system simply requires that the dApp be able to look up the contract and verify its existence.

    b. Verification: The dApp verifies the validity of the contract on the associated blockchain.

3. Jiritsu Contract Integration: The contract identifiers are registered on the Jiritsu contract, which is then immutably bonded with the data representing the proof.

Glossary

- **Claim:** An action taken by the Tokenizer that will connect their on-chain tokenized RWA to the related data on the Jiritsu Ledger.
- **Verifier:** A script or code that is run by ZKMPC nodes in order to verify a workflow.
- **Proof Provider:** Provides a Verifier uploaded to Jiritsu ZKMPC nodes in order to generate a proof to the JiriLedger that is of interest to Tokenizers.
- **Proof Provider Connector:** The software that connects the Jiritsu Ledger dApp to the Proof Provider
- **Jiritsu dApp:** A web application provided by Jiritsu that:
    a. Allows Tokenizers to claim proofs for their on-chain data
    b. Enables Proof Providers to upload their data to the Jiritsu Ledger
- **Jiritsu Ledger:** An L1 blockchain maintaining cryptographic proofs of Real World Assets and their related data.
- **Jiritsu Proof:** A cryptographic proof created for the data of a Real World Asset by the Jiritsu ZKMPC platform that is written to the Jiritsu Ledger
- **Tokenizer:** The issuer of tokens of a Real World Asset (RWA).

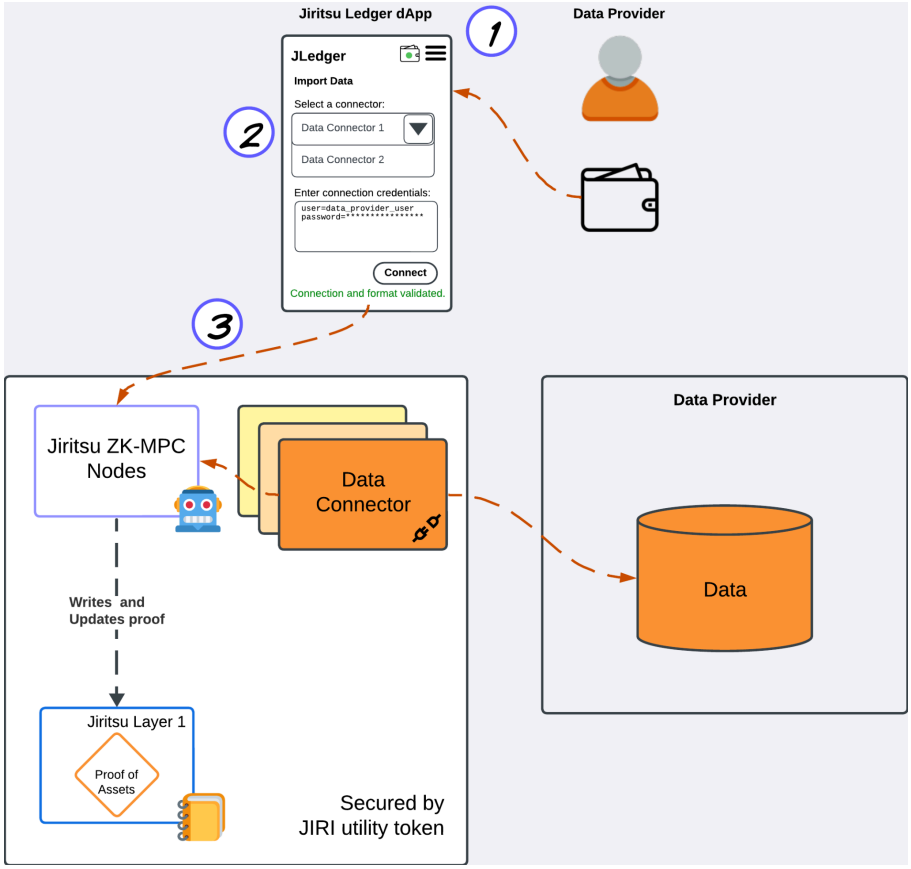
Prerequisites

1) For Proof Providers
    a) The Proof Provider must have a crypto wallet.
    b) A configured and tested Proof Provider Connector for your data.
2) For Claiming
    a) For the asset you wish to claim, you'll need the on-chain contract details
        i) Blockchain: Which blockchain is it located on.
        ii) Address: The address of the contract.
    b) Claiming Key: This is a secret token provided to the asset owner by a data provider ensuring the owner is the one claiming proofs of ownership.
    c) As the asset owner, determine ahead of time if you'd like to keep the proof data private (encrypted) or not.

Importing Proof onto the Jiritsu Ledger

The following describes the process for Proof (Data) Providers to upload their Proof onto the Jiritsu Ledger:

1) Proof Provider connects to the Jiritsu Ledger dApp with their crypto wallet.
2) Proof Provider chooses the appropriate Verifier that will connect to the data.
3) Once connected successfully, the Verifier will validate the data format and generate the the proof which is imported onto the Jiritsu Ledger.
4) **Optional**: The Data Provider can grant access to view the data by adding wallet addresses to the allowed-access list



Claiming data on the Jiritsu Ledger

1) Tokenizer wishing to claim data connects to the Jiritsu Ledger dApp with their crypto wallet.
    a) Tokenizer searches and locates the data entry on the ledger.
    b) Tokenizer clicks to claim the data entry.
2) Tokenizer provides the token's contract details by providing which blockchain it's on and the contract address.
    a) The dApp will attempt to connect to the contract and validate it.
3) Once the contract is validated, the claim request is submitted to the Proof Provider
4) The Proof Provider receives the Claim request and approves it
5) The dApp requests the Jiritsu ZK-MPC platform to associate data from the Proof Provider to Tokenizer as the "Claimer" with the contract address located on the blockchain provided.