Universal Digital Payments Network

User Manual

September 1, 2022
Version V1.0.2

Document Information

Document Name	Universal Digital Payments Network User Manual
Author	Miaomiao Xu
Last Updated	August 31,2022

Change Records

Version	Date	Change Notes	Modified by
V1.0.0	2022-05-26	Create	Miaomiao Xu
V1.0.1	2022-07-05	Replace screenshots and adjust format	Miaomiao Xu
V1.0.2	2022-09-01	Screenshots and text updates	Olivier Truquet

Document review

Name	Post	Sign	Date

Delivery Approval

Name	Post	Sign	Date

Catalogue

1. UDPN Introduction

Scalable and universal interoperability will enable efficient and smooth movement between the legacy payments infrastructure and the rapidly evolving digital currency infrastructure. The Universal Digital Payment Network (UDPN) addresses this issue by creating a global payment network designed for regulated fiat-backed stablecoins and CBDCs across decentralised and centralised systems.

There is an opportunity to unify the fragmented ecosystems, leveraging Blockchain infrastructure advances and connecting regulated fiat-backed stablecoins and centralised CBDCs. The goal of the UDPN is to create a shared, decentralised network and associated standards to improve cross-border payment processing efficiency. The UDPN enables enterprises from different countries to transact and settle in foreign currencies by merely accessing their Business Nodes installed locally. Furthermore, the UDPN provides a way for commercial banks and regulated businesses to participate in the digital economy.

Just as the SWIFT network (linking more than 11,000 financial institutions across 200 countries and territories) created the original standard for messaging between financial institutions across different settlement systems, the UDPN will serve the same purpose for the emerging generation of CBDCs and stablecoins. By leveraging enterprise DLT blockchain technology for multi-party coordination and using smart contract frameworks to automate settlement and compliance processes in all digital currency systems, the UDPN will lead the way in the next global financial settlement era.

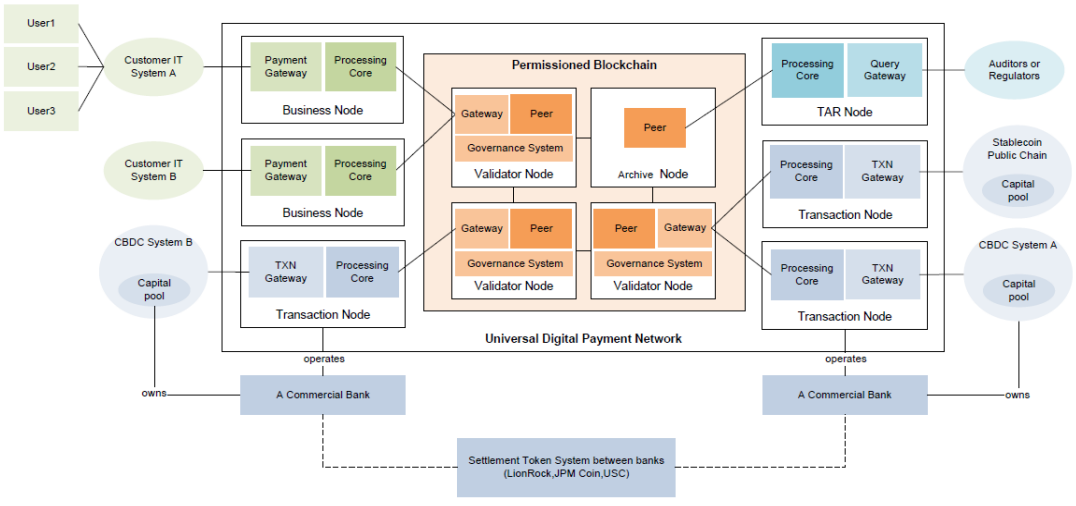
Unlike most other digital currency projects, the UDPN will not issue any central token to be circulated on the network for settlement purposes. Instead, the UDPN will operate more like an inter-currency network, working with multiple stakeholders and becoming the messaging backbone between various CBDC and stablecoin systems.

A key challenge to achieving a common international infrastructure for cross-border payments centres around creating a robust governance model. Specifically, one which allows stakeholders from all countries to participate in the use, development, operation, and maintenance of the network, in a trusted and equitable way. Therefore, the goal of the UDPN is to develop an inclusive framework to address the issues of governance, ownership, and participation in a network leveraging DLT Blockchain technology. To achieve this goal and overcome the challenges in cross-border payments' governance, the UDPN will be managed by an alliance of financial institutions and technology companies from different countries and industry verticals, each having shared ownership of the network.

2. Explanation of Terms

- **Blockchain:** a new application mode of computer technology including distributed data storage, point-to-point transmission, consensus mechanism, and encryption algorithm
- **IT System:** interface through which the end user initiates transfer or swap transactions
- **Business Node (BN):** gateway to the UDPN which is owned and set up by third-party businesses who wish to integrate UDPN services into their business systems
- **Transaction Node (TN):** custom-made software executing validated transactions on the UDPN in their respective digital currency systems
- **Validator Node (VN**): on-chain node connecting all other stakeholders via a secure and encrypted connection to validate any transaction on the UDPN and provide services such as smart contract deployment for Business Nodes and Transaction Nodes
- **Transaction Audit and Reporting (TAR):** on-chain node storing all the block ledger data on the network and facilitating the work of regulators and auditors when monitoring transactions on the network

3. UDPN High-Level Architecture



The primary objective of the UDPN is to provide a messaging infrastructure for global cross-border

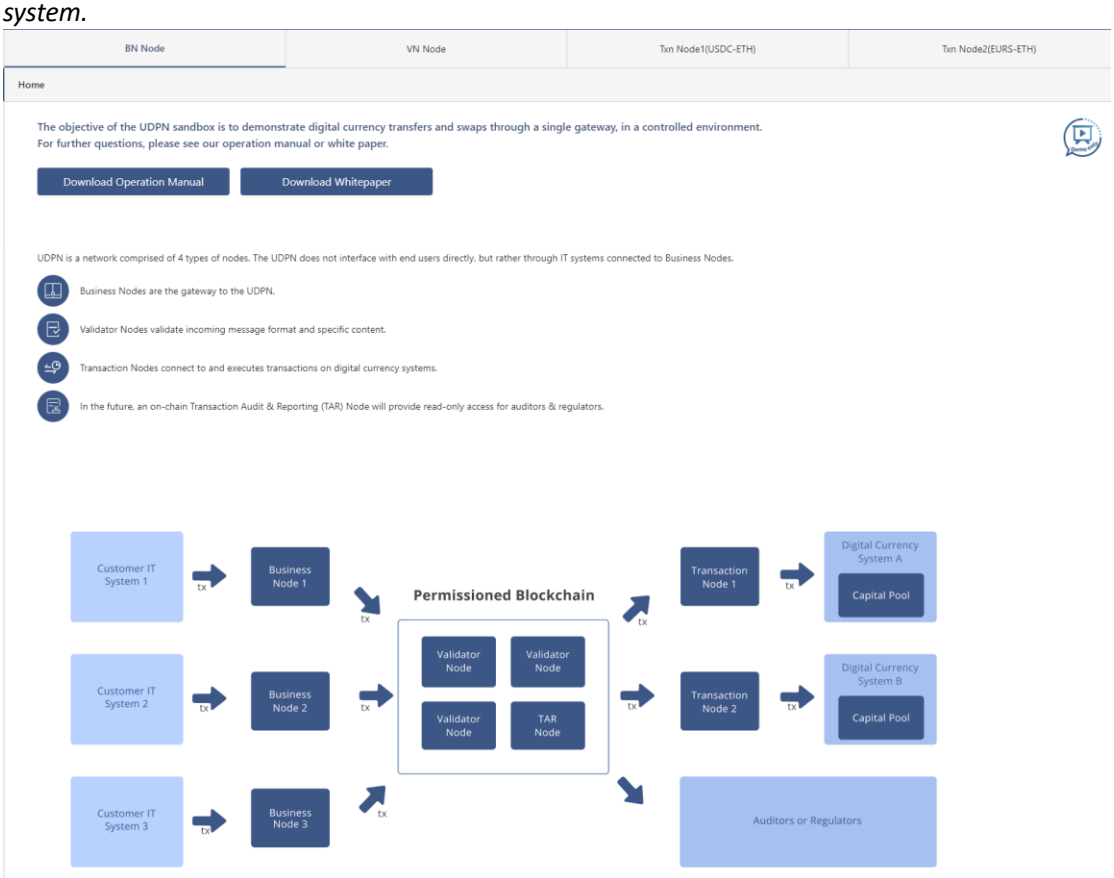
payments of regulated fiat-backed stablecoins and CBDCs. With most businesses being off-chain, the UDPN infrastructure connects businesses' IT systems with stablecoin and CBDCs currency systems, using Hyperledger BESU as the permissioned framework.

The architecture is a permissioned, decentralised network of Validator Nodes (on-chain), which communicate with Business and Transaction Nodes (off-chain). Transaction Nodes operated by regulated institutions securely connect to digital currency systems, while Business Nodes allow any businesses' IT systems to connect to the UDPN. Finally, the on-chain Transaction Audit and Reporting Node facilitates the work of Regulators and Auditors in monitoring transactions of their respective digital currencies.

4. Home

The **Home** page introduces the main objectives of the Sandbox and the UDPN infrastructure. Users can click the "Download Operation Manual" or "Download Whitepaper" buttons to download the relevant documents.

This UI is for demonstration purpose only and will not be implemented in the UDPN production system.



Note: Three icons "Demo only", "WEB", and "API" are placed on different pages of the UDPN Sandbox website and are described below:

1) Demo only: this page is for demonstration purpose only and will not be implemented in production

2) Web: this page is available for the user via a Web page in the UDPN production system

3) API: this function will be provided to the UDPN user via an API in production.

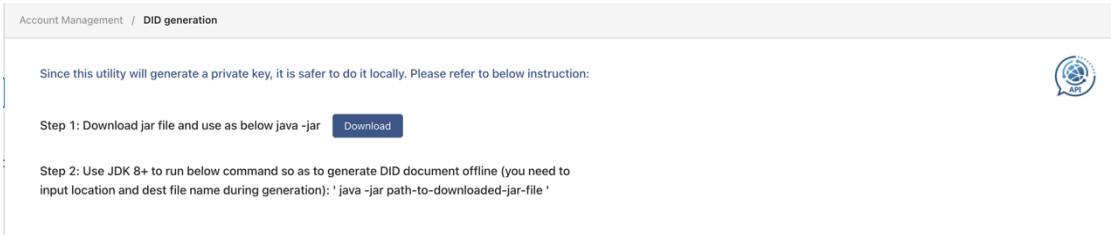
5. Account Management

5.1 Overview

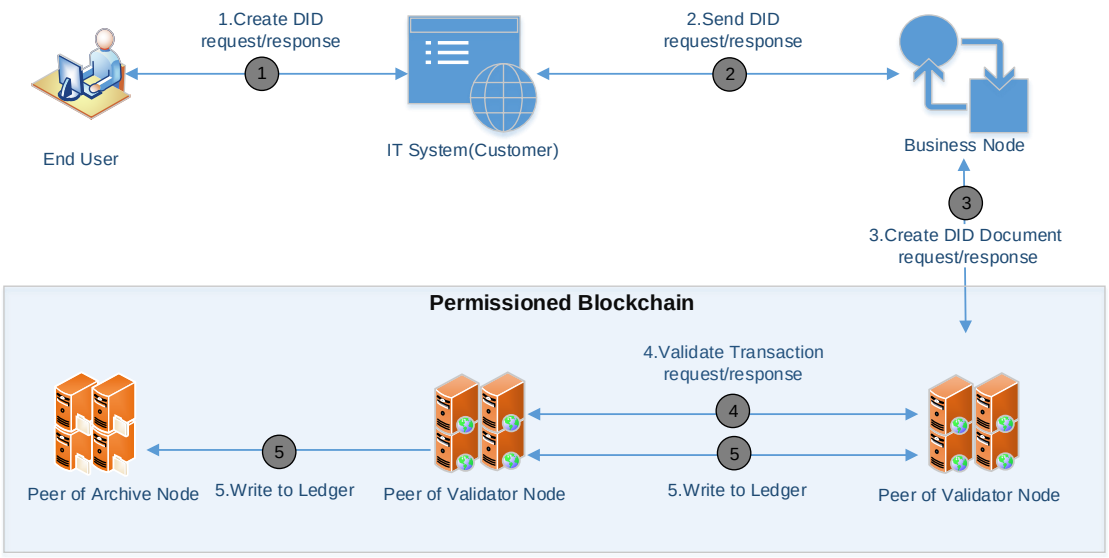
The **Account Management** page provides access to various UDPN functions such as creating a DID, linking a digital currency account to a DID, and linking a business account to a UDPN DID.

5.2 DID Generation

The **DID Generation** page describes how IT systems can generate DIDs and their corresponding private keys offline on behalf of end-users. In production, IT systems will be able to generate DIDs offline via a dedicated API.

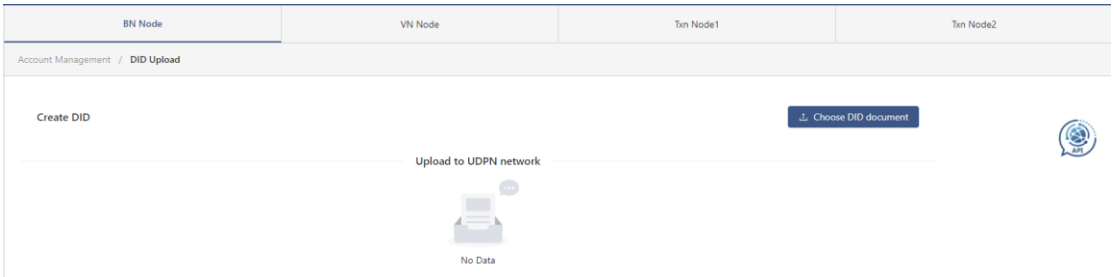


To generate a DID:



5.3 DID Upload

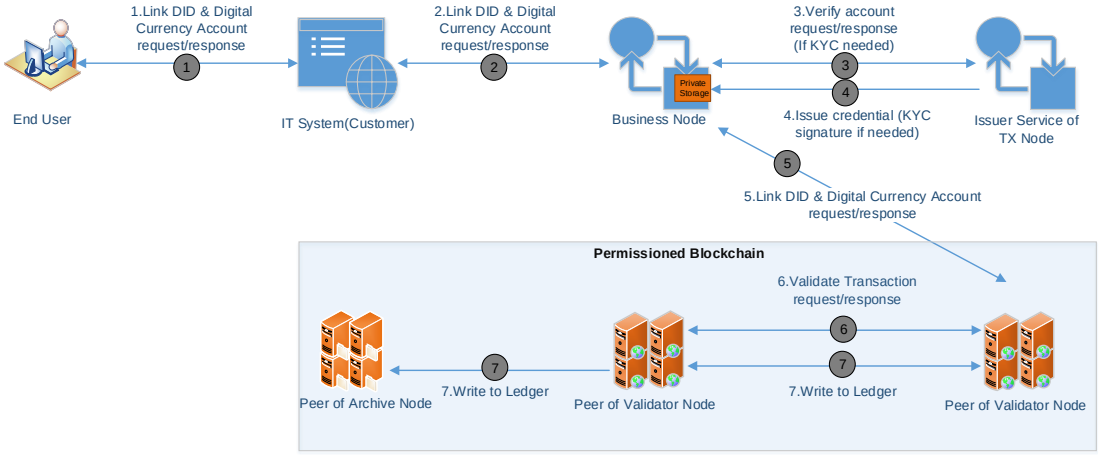
The **DID Upload** page displays how to upload the DID document generated. In production, Business Node operators can complete this operation via a dedicated API.



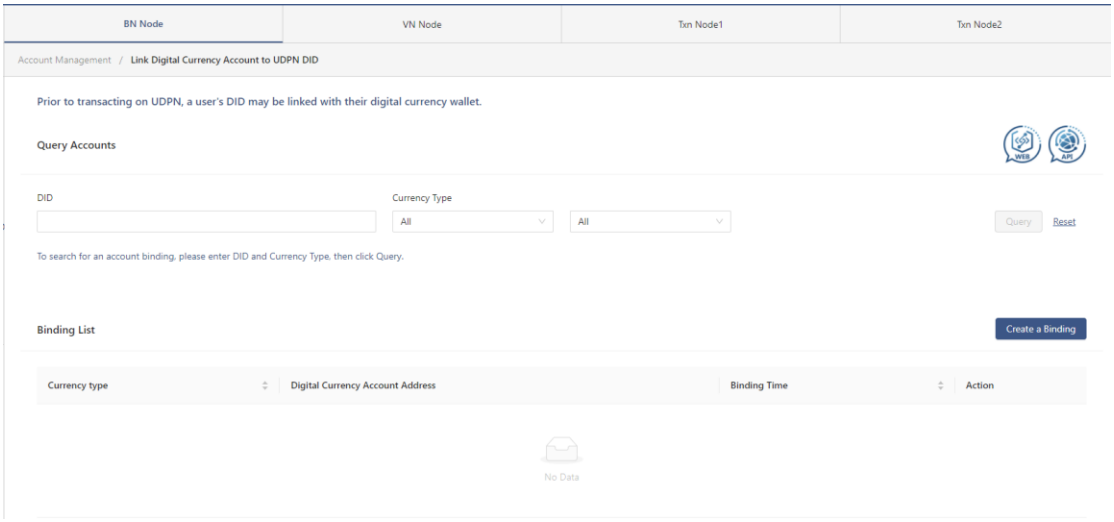
5.4 Link a Digital Currency Account to a UDPN DID

A user must bind their DID with a digital currency account before transacting on UDPN. In production, users will link their DID to digital currency accounts via a Web interface or a dedicated API.

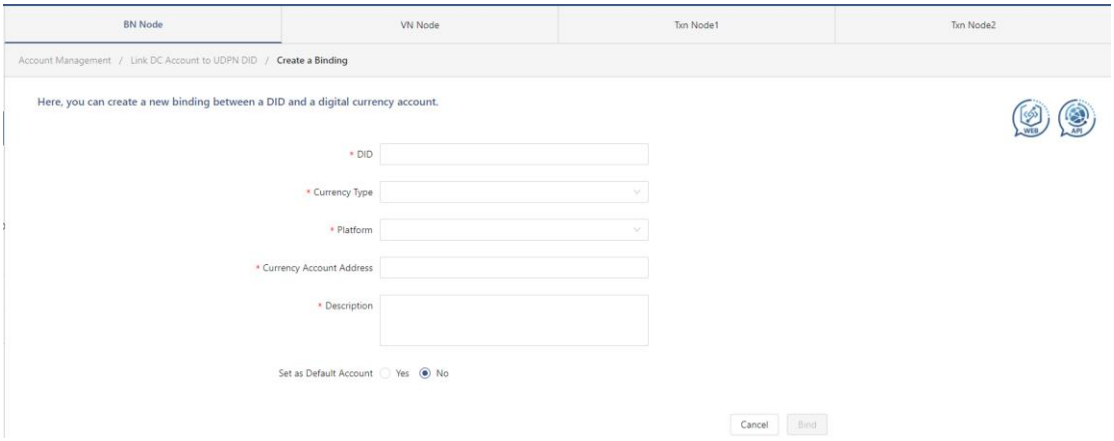
The process for linking a digital currency account to a UDPN DID is as follows:



Click on the "Account Management" menu, then click on the "Link Digital Currency Account to UDPN DID" sub-menu to arrive on the page displayed below:



- Next, click on the "Create a Binding" button to go to the page displayed below:

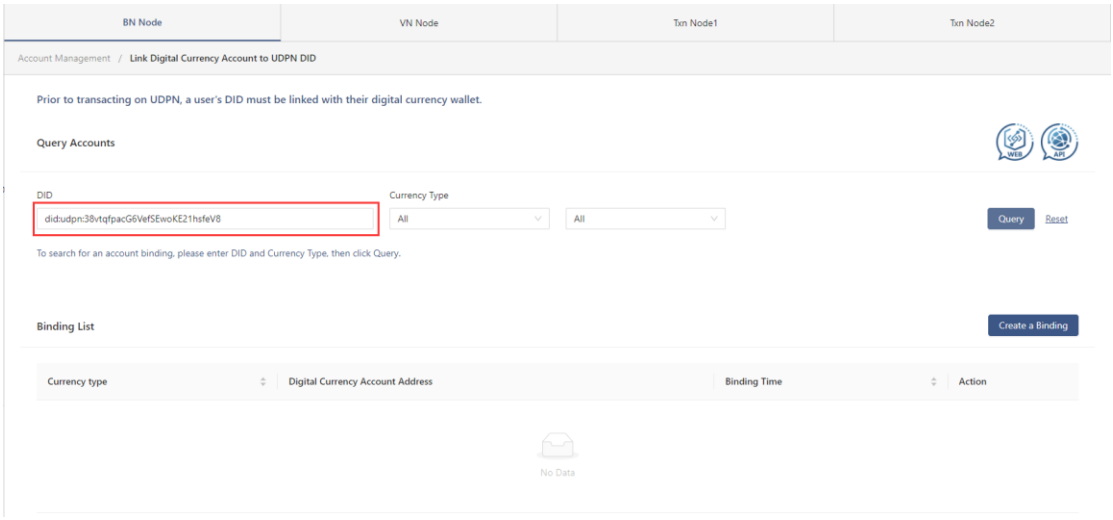


- Fill in the form as follows:
    1. Enter your DID
    2. Select the currency type
    3. Select the platform (Blockchain) to connect
    4. Enter your digital currency account number (or address)

5. Include a simple description
6. Select whether the digital currency account should be used as your default account. You can only select one default account per currency and digital currency system
7. Click "Bind" to complete the DID and account linking operation

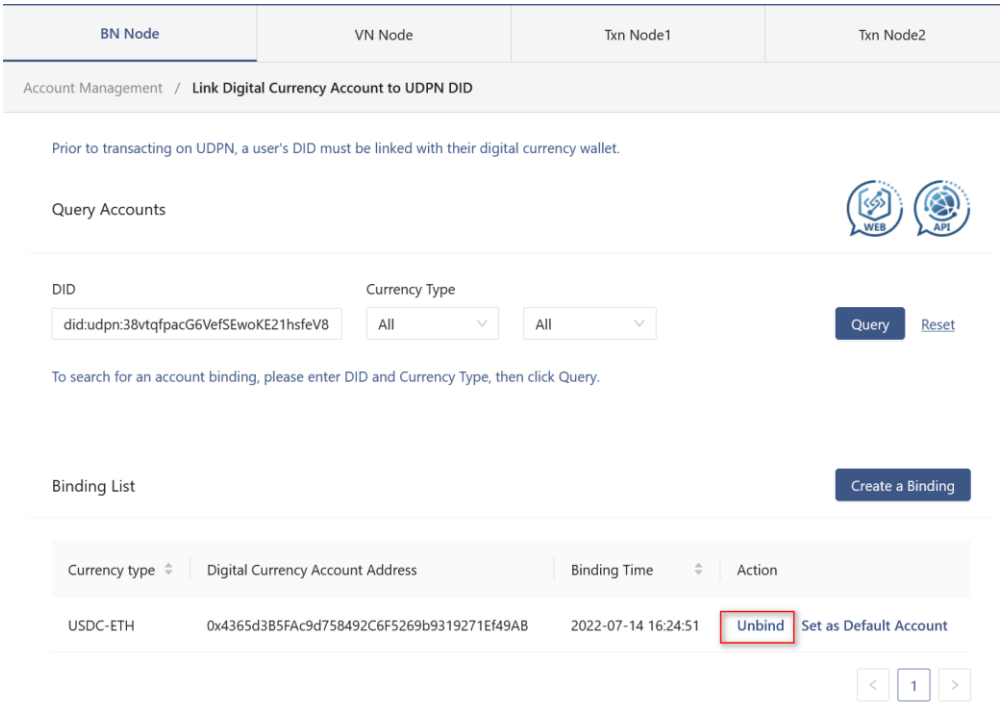
- To make a DID Query:
    1. Enter a DID. Make sure to enter the DID correctly
    2. Select the currency type
    3. Click on the "Query" button to retrieve all relevant linking information regarding the DID and the chosen currency

  Note the "Currency Type" dropdown menu is set to “All” by default to show all digital currencies linked to the desired DID.



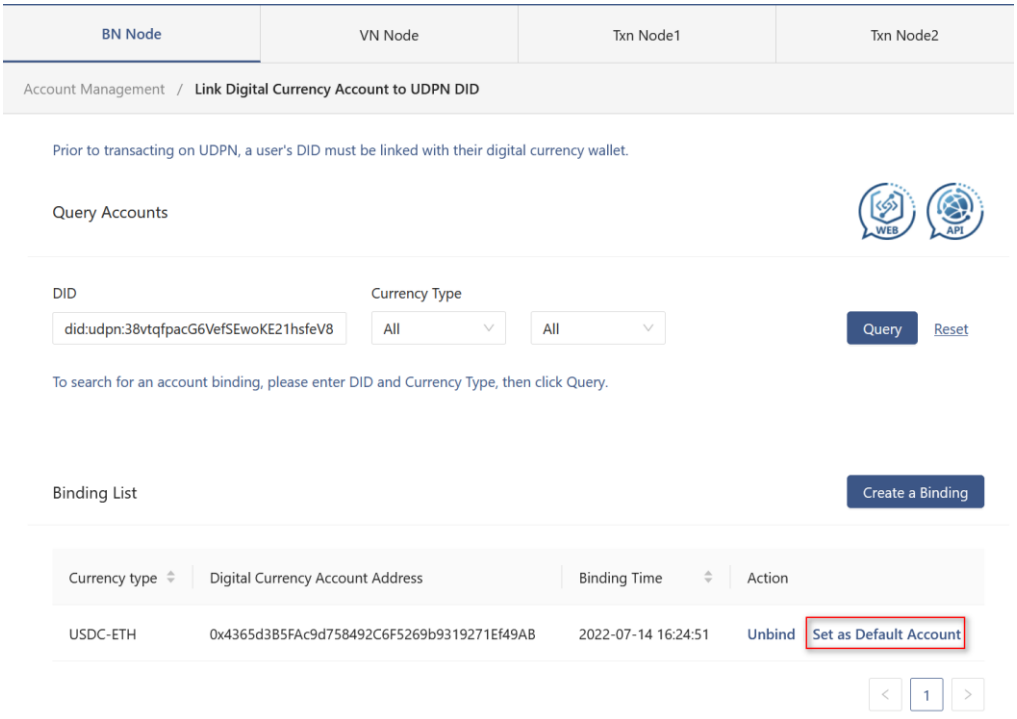
- To "Unbind" a digital currency account from a DID:
    1. Enter the desired DID
    2. Click the "Query" button to review all accounts linked to the desired DID
    3. Select the linked account you want to unbind and click on the "Unbind" button
    4. Confirm your decision to unbind the DID and the digital currency account

  Upon confirmation, the DID and digital currency account will no longer be linked. Therefore, you will no longer be able to use this account on the UDPN.



- Set an existing account as "Default" (assuming a digital currency account is already linked to the desired DID):
    1. Enter the desired DID in the search box
    2. Click on the "Query" button
    3. Select the account you want to set as your default account by clicking the "Set as Default Account" button

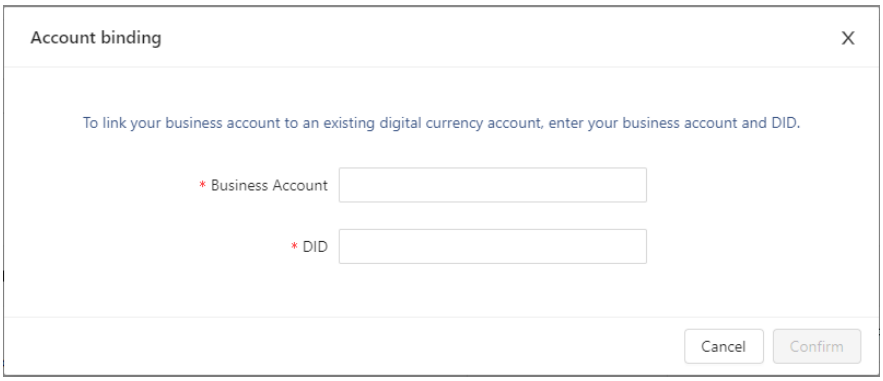
  If there is an existing default account for a given currency and platform, the existing account will be overwritten.



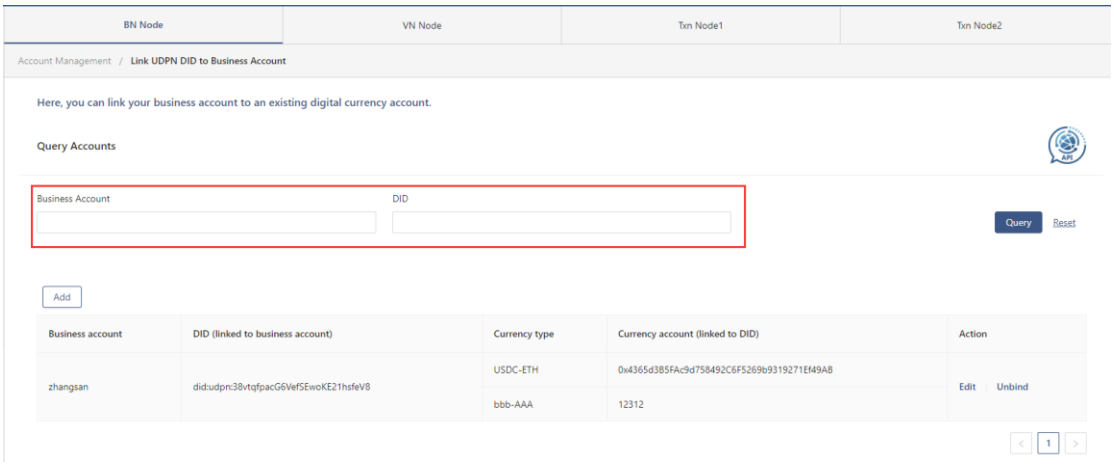
5.5 Link a UDPN DID to a Business Account

Business Accounts are the equivalent of external identifiers. For example, a bank account number could be used as a "Business Account" on UDPN and linked with DIDs. The UI will display DIDs and their linked business accounts in a table (shown below). In production, users will be able to bind their Business Accounts with their DID via a dedicated API.

- To link a DID with a Business Account:
    1. Click on the "Link UDPN DID to Business Account" menu
    2. Click on the "Add" button to open an “Account Binding” pop-up window
    3. Enter the desired Business Account name
    4. Enter the desired DID
    5. Click on the Confirm button to link the desired DID to the desired Business Account. A user can bind any business account to their DID



- To make a Business Account & DID query:
    1. Enter the desired Business Account in the textbox displayed below
    2. Enter the desired DID in the textbox displayed below
    3. Click on the "Query" button



- To edit a binding, proceed as follows:
    1. Select the desired DID and business account you want to edit from the table on the "Link UDPN DID to Business Account" page
    2. Click "Edit"
    3. Make any desired change and confirm

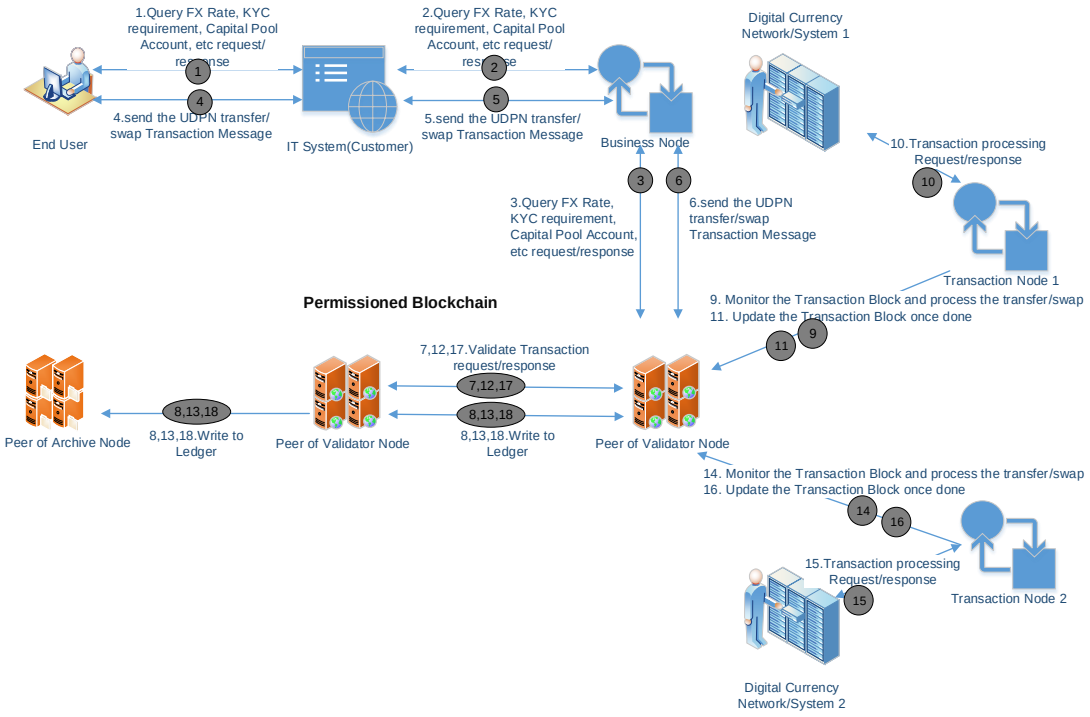
- To "Unbind" a Business Account from a DID, proceed as follows:
    1. Select the linked DID and Business Account you would like to unbind from the list on the "Link UDPN DID to Business Account" page
    2. Upon clicking "Unbind," the UI will no longer display unbound data in the table

6. Transaction Management

6.1 Overview

The **Transaction Management** Page facilitates the execution Transfer/Swap transactions and queries of relevant transaction information.

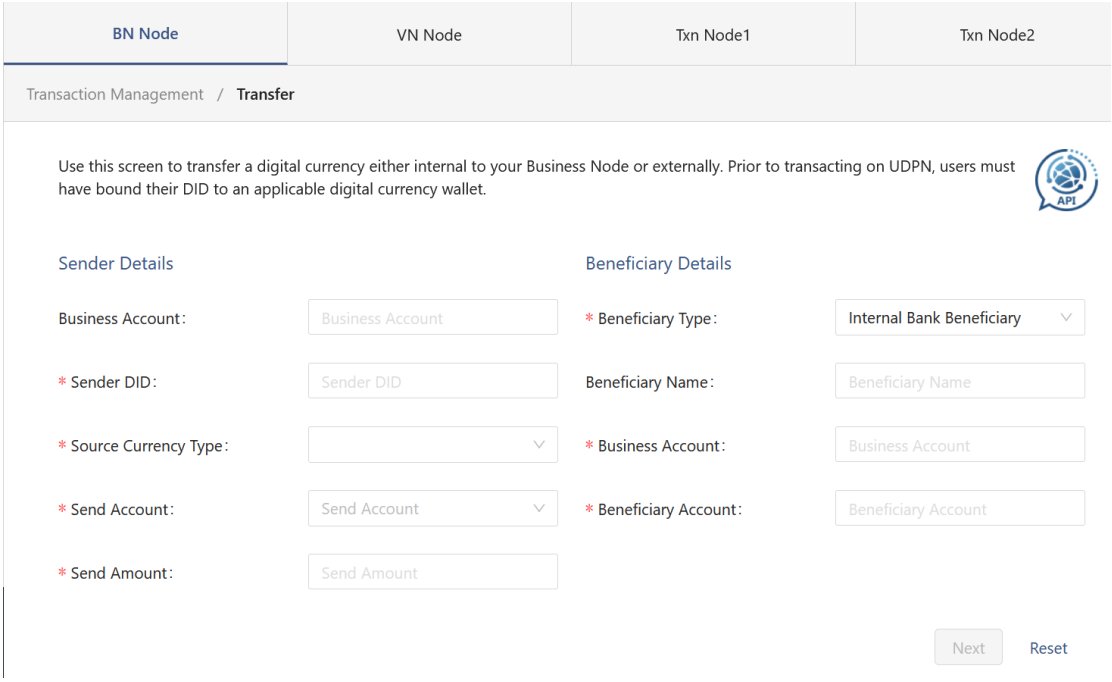
Please refer to the diagram below to familiarize yourself with transfers and swaps on the UDPN:



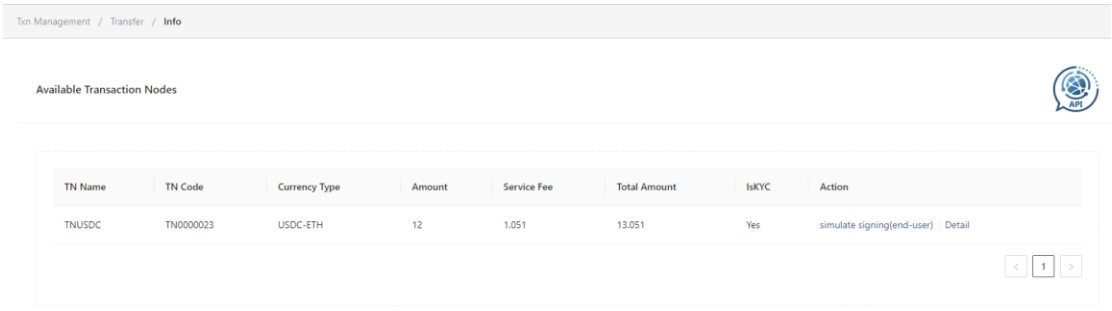
6.2 Transfer

The Transfer page simulates how IT Systems complete transfers on behalf of end users.
It also illustrates a complex linking scenario. In this scenario, a DID is linked to both a Business Account (e.g., a bank account), and a digital currency account. Entering the Business Account allows the system to auto-fill most of the information required.

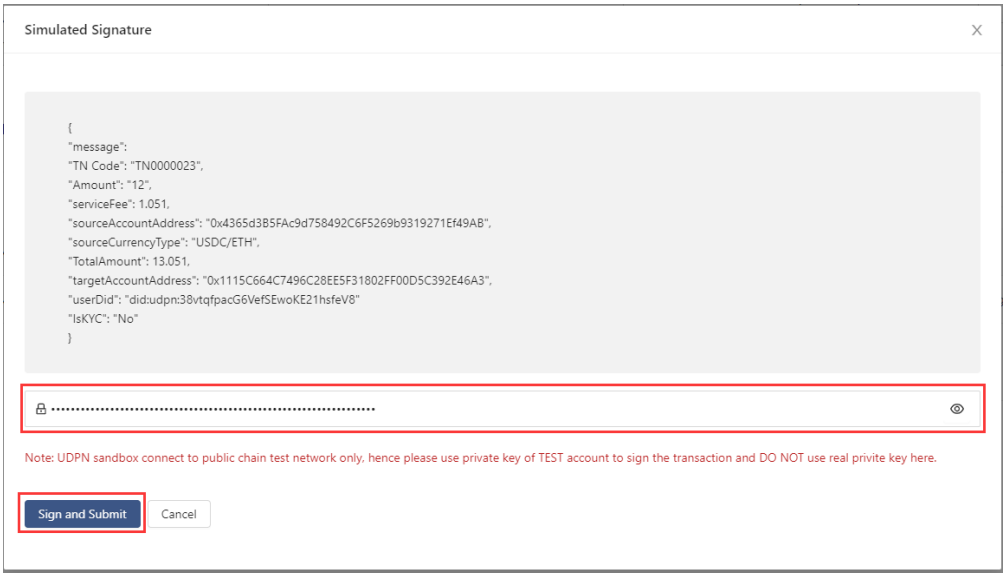
In production, this function will be accessible via a dedicated API.



- Complete the Sender Details:
    1. Input the Business Account and Sender DID
    2. Select the currency type and input the Sender Account and the sending amount
    3. Complete the Beneficiary Details. Select Beneficiary Type, specifying whether the beneficiary is an Internal Client or an External Beneficiary. If the Beneficiary Type is an Internal Bank Beneficiary, enter the Beneficiary Name and associated Business Account
    4. Enter the associated Beneficiary Account
    5. Click the "Next" button to go to the next page

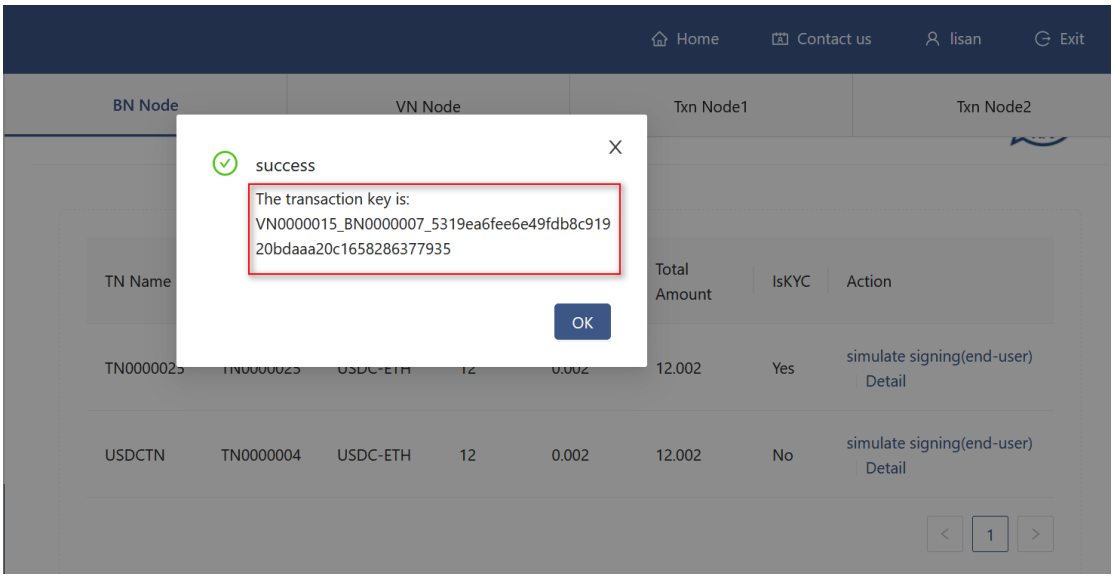


- How to simulate a signature from an end user’s perspective: The sender must sign a transfer transaction for the transaction to be executed. After clicking the "Simulate Signing" button, the Sandbox will simulate a signature request.

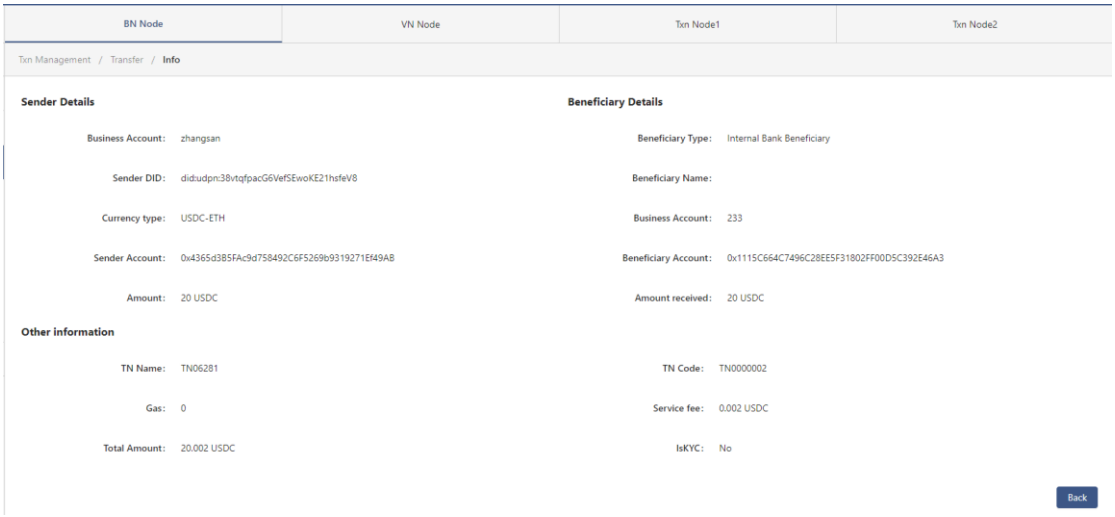


The end user must enter their private key (starting with 0x) in the above interface and then click the "Sign and Submit" button to submit the transaction for execution.

After the transfer transaction is successful, you will get a unique transaction key that you can use to query for the transaction. Save this key in a secure location to query the transaction information.

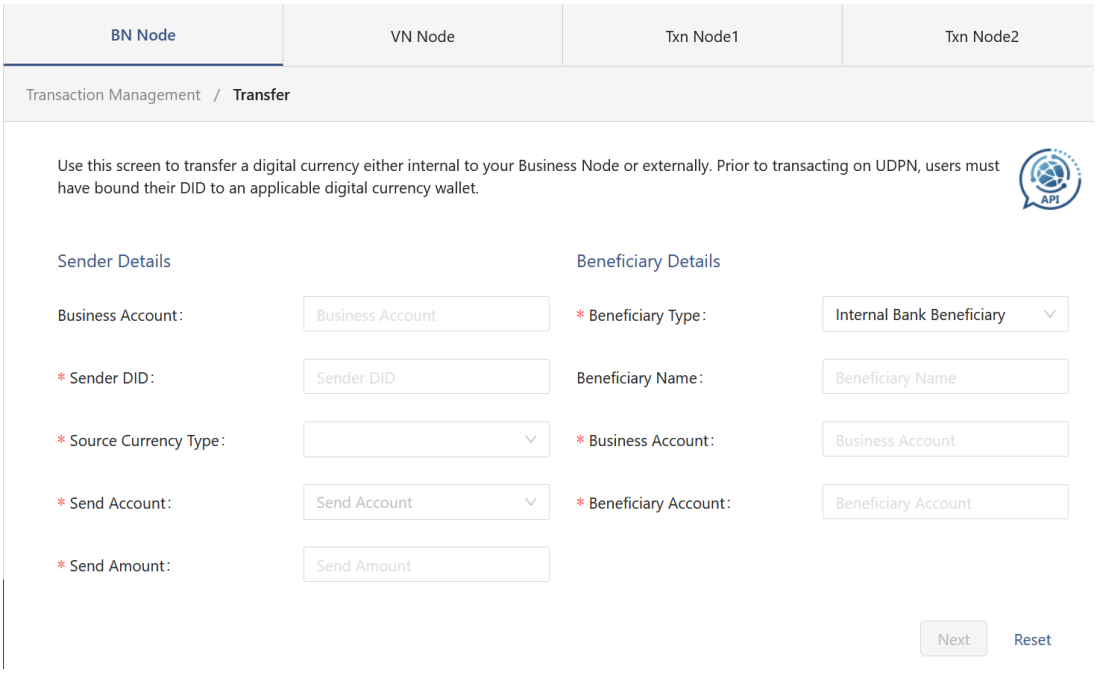


- **Detail**: displays the transfer details, such as Sender and Beneficiary Details.



6.3 Swap

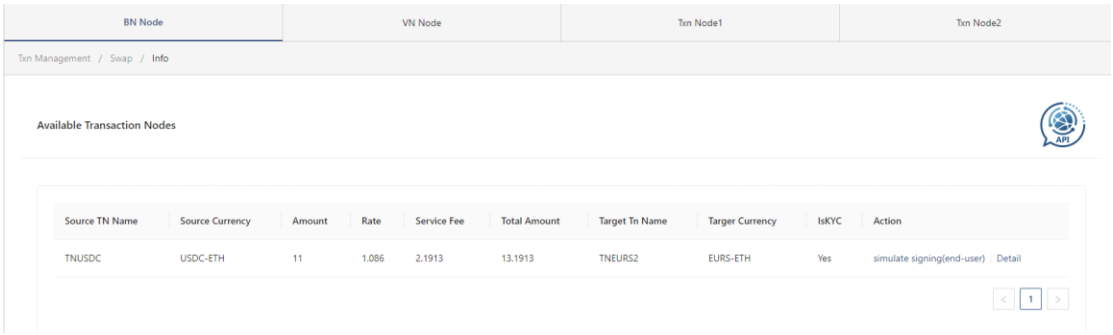
The **Swap** page shows how IT systems can complete digital currency swaps on behalf of end-users. In production, this function will be accessible via a dedicated API. In the scenario below, the bank account used as a Business Account is linked to a UDPN DID. This UDPN DID itself links to a digital currency account. Entering the Business Account allows the system to auto-fill most of the information required. The connected digital currency account can also be displayed automatically upon selecting a currency type in the drop-down menu.



- To complete a swap on the UDPN:
    1. Complete the Sender Details by entering the Business Account and Sender DID.
    2. Select a Source Currency Type from the dropdown menu
    3. Enter the Sender Account and Amount to send
    4. Select the Beneficiary Type from the relevant dropdown menu (selection options include Internal Bank Beneficiary and External Beneficiary) and a Target Currency Type from the appropriate dropdown menus

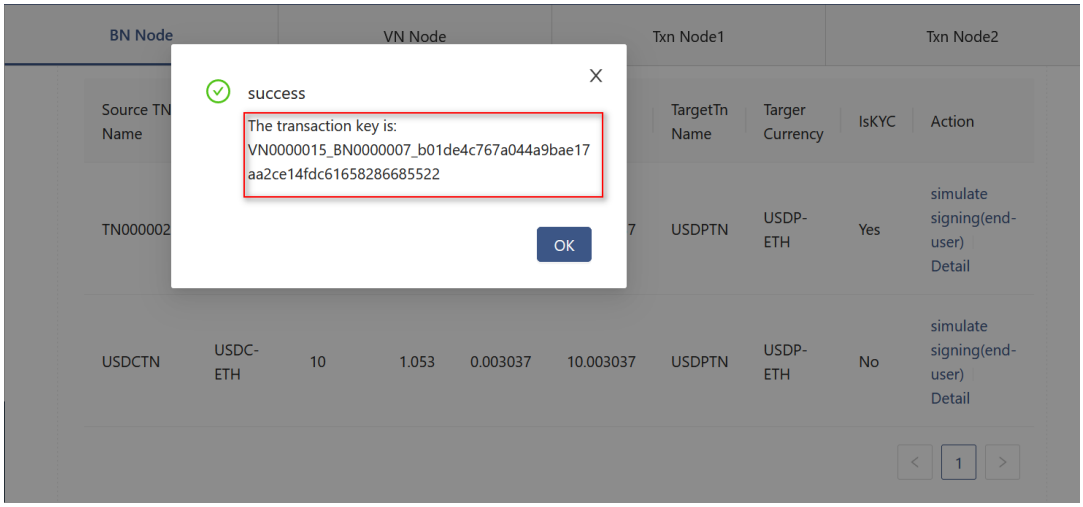
5. Input the Beneficiary Account
6. Click on the "Next" button to jump to the next page

Please note that the Beneficiary Name and Business Account fields will only be available when the Beneficiary is an Internal Bank Beneficiary.

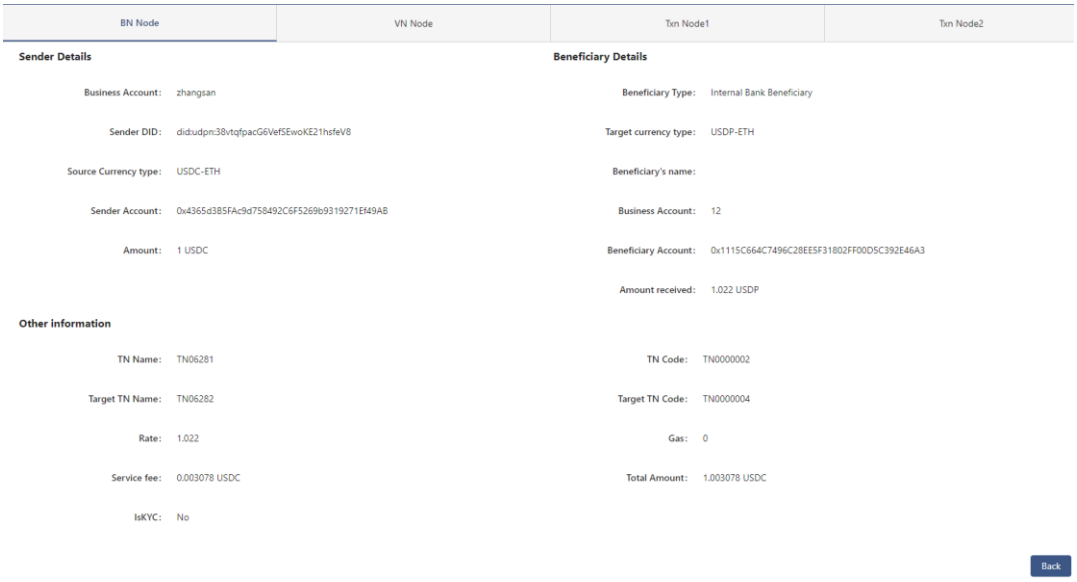


- How to simulate a signature from an end user's perspective: The sender needs to sign a swap transaction for the transaction to be executed.
    1. Click on the "Simulate Signing" button
    2. Enter your private key (starting with 0x) in the above interface and then click the "Sign and Submit" button to submit the transaction for execution

After the swap transaction is successful, a unique transaction key will be generated. Save this key in a secure location to query the transaction information.

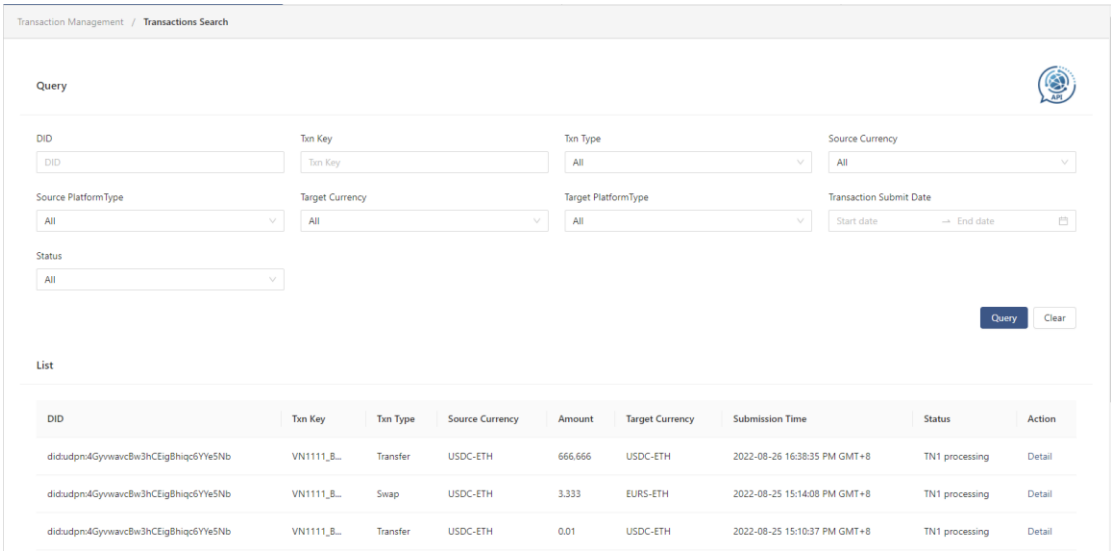


- **Detail**: used to display the details of a transfer, including Sender and Beneficiary Details

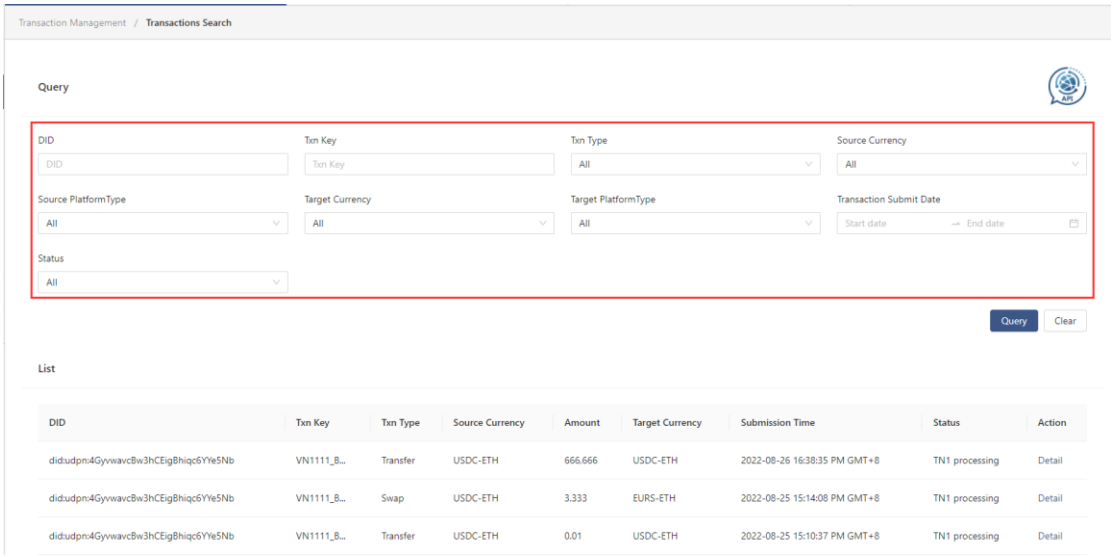


6.4 Transactions Search

The **Transactions Search** page demonstrates how users can query transaction information via their IT system. In production, this function will be accessible via a dedicated API.



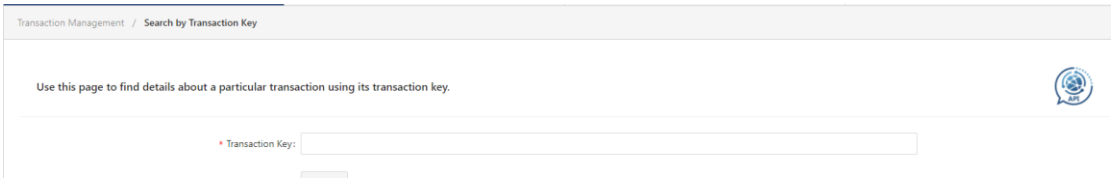
- Query transaction information:
    1. Enter the desired DID and Transaction keys
    2. Select the Transaction Type, Source Currency, Target Currency, Transaction Submit Date, and Status
    3. Click on the "Query" button. The search results will be displayed in the Transaction table below the Transaction Query Section



- View details: Transaction details include primary sender/beneficiary information and transfer/settlement information
    1. Choose one of the transactions in the Transaction List
    2. Click on the "Detail" button to view the transaction details.

6.5 Search by Transaction Key

This page shows how IT System users can query a transaction's information using a Transaction Key. In production, this function will be accessible via a dedicated API.



- **Query**:

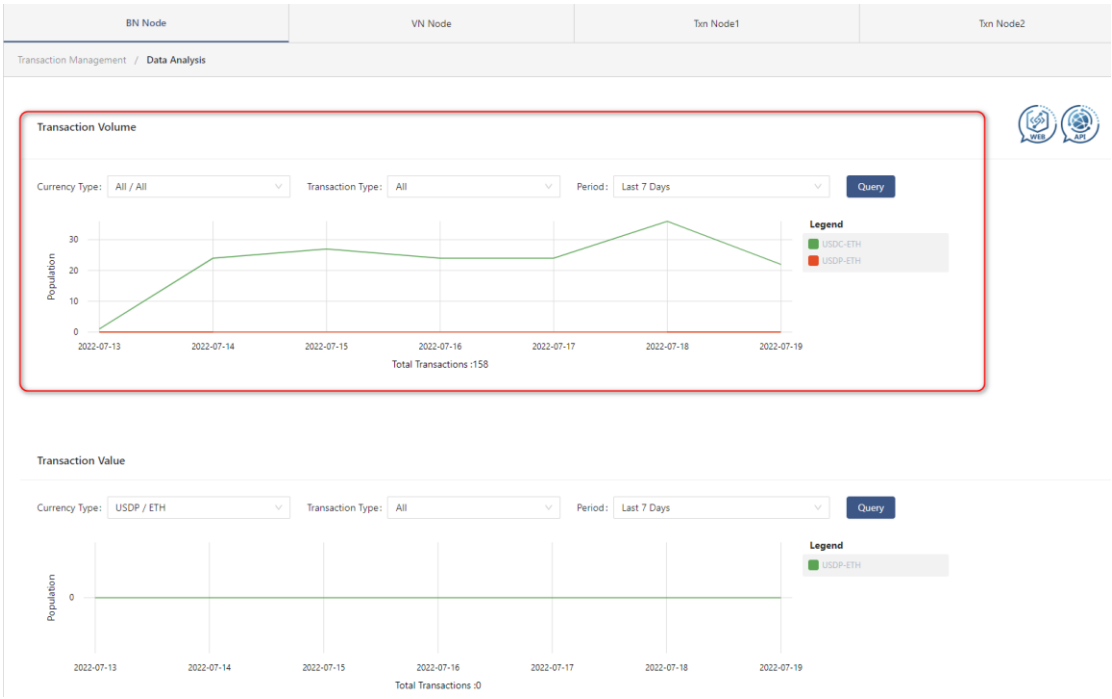
    1. Enter the desired Transaction Key
    2. Click on the "Query" button to go to the "Transaction Details" page, which displays the primary sender and beneficiary information as well as the transfer and settlement information

6.6 Data Analysis

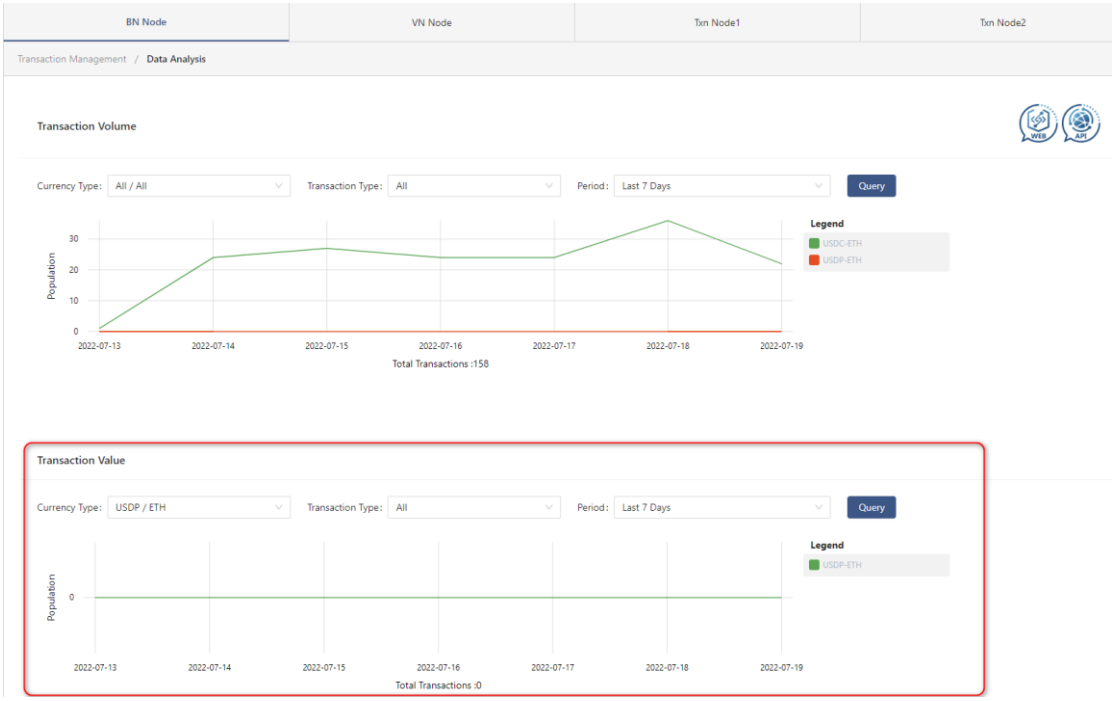
The Data Analysis Page displays the number and volume of transactions processed in the past 7 or 30 days based on the different currencies and transaction types. This function will be accessible via a web interface or a dedicated API in production.

- Transaction Volume: After selecting the currency type, transaction type and period of

interest, click the "Query" button to see the total number of transactions in the past 7 or 30 days.



- Transaction Value: After selecting the currency type, transaction type and statistical period, users can click "Query" to query the total transaction value of a particular currency in the past 7 or 30 days.



7. Network Access Configuration

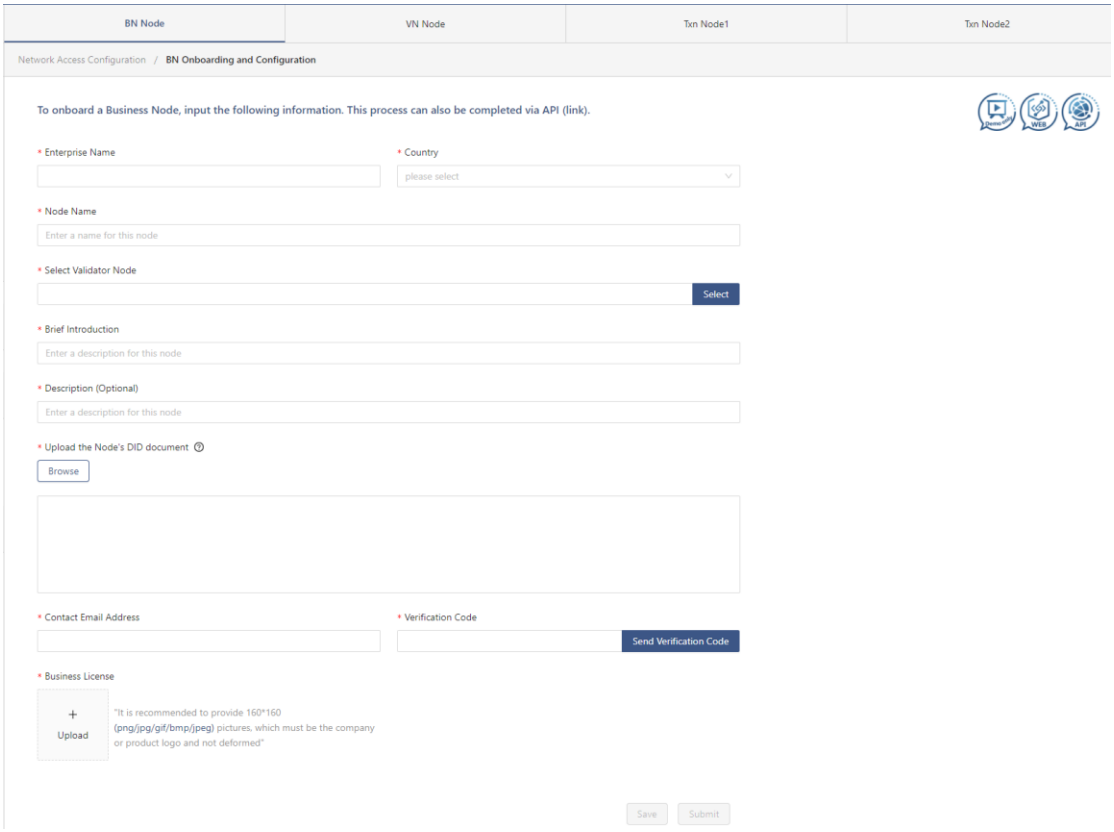
7.1 Overview

The **Network Access Configuration** page allows the BN operator to access the UDPN network and digital currency systems supported by the UDPN network. A BN operator must provide information such as its enterprise name, country, node name, connected VN, locally generated DID (see section 5.2), contact email and business license to access the UDPN Network. The **Digital Currency Access** page shows the digital currencies available to IT systems via the BN Node gateway and the future currencies that will be supported on the UDPN.

In the current sandbox, the Network Access Configuration and Digital Currency Access pages are for demonstration purpose only and are not functional. In production, a BN administrator will be able to complete the BN Node network access and configuration via a secure website or via APIs supported by VNs.

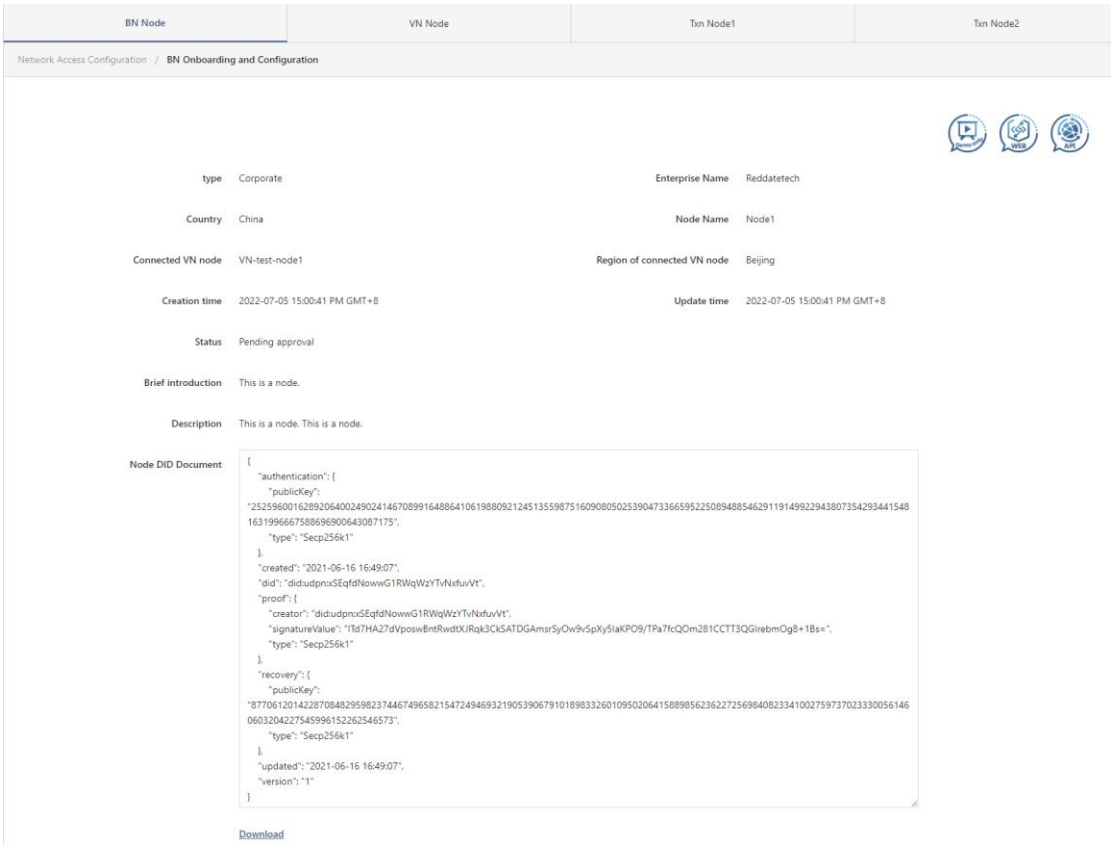
7.2 BN Onboarding and Configuration

To apply for UDPN access as a BN operator, a user can click on the "BN Onboarding and Configuration" tab in the pull-down menu for "Network Access Configuration:"



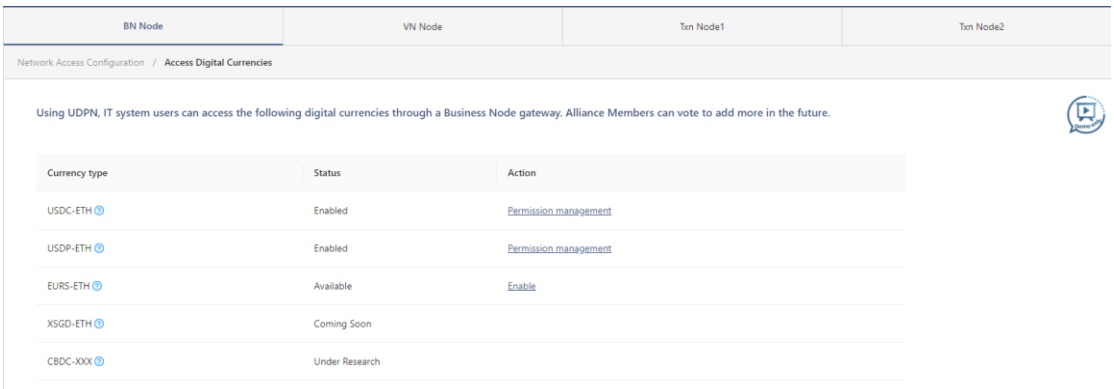
- Enter the relevant BN information (including enterprise name, country, node name, connected validator node, DID, contact email, business license) and click "Submit."

- After applying for Business Node access to the UDPN network, the Validator Node operators will vote on granting UDPN access to the BN applicant. Upon approval, the Business Node information will be displayed as shown below:

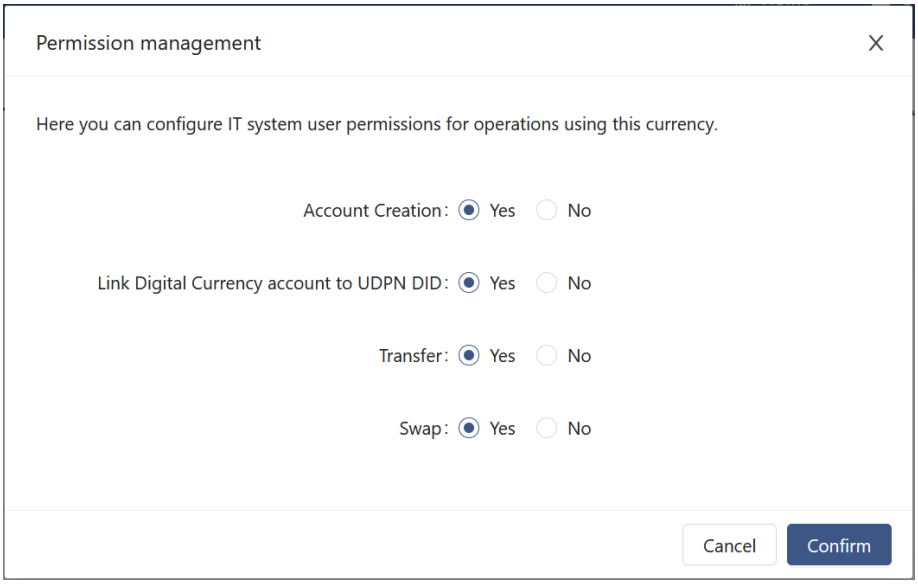


7.3 Access Digital Currencies

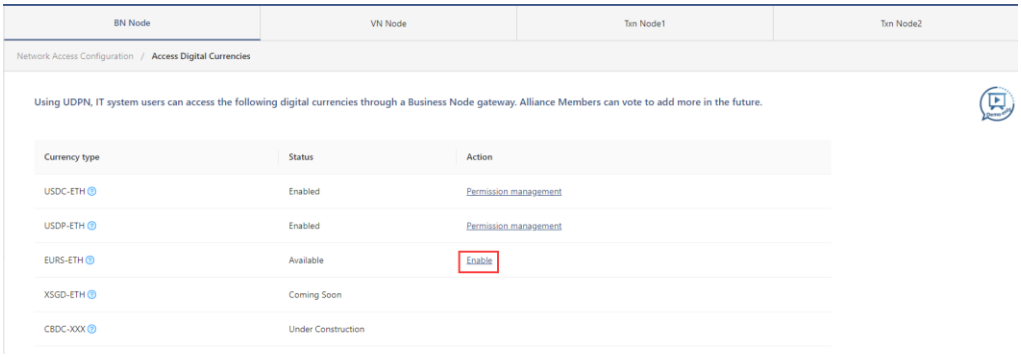
The BN Operator can click "Access Digital Currencies" in the pull-down menu for "Network Access Configuration" to display the "Access Digital Currencies" sub-page:



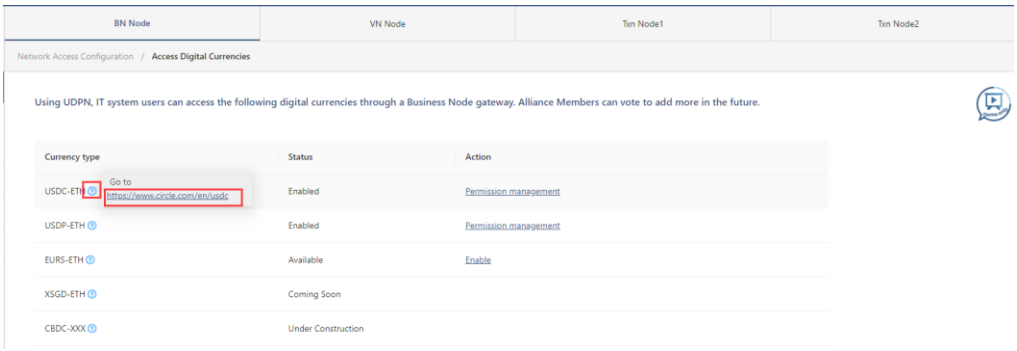
- The BN Operator can click "Access Digital Currencies" in the pull-down menu for “Network Access Configuration" to display the following page:



- Enable: If the UDPN supports a currency, but the IT system users are not allowed to use it, click "Enable" here will make it available to them.



- Users can click "Help" to direct to the official website of the currency that is or will be supported by the UDPN network.

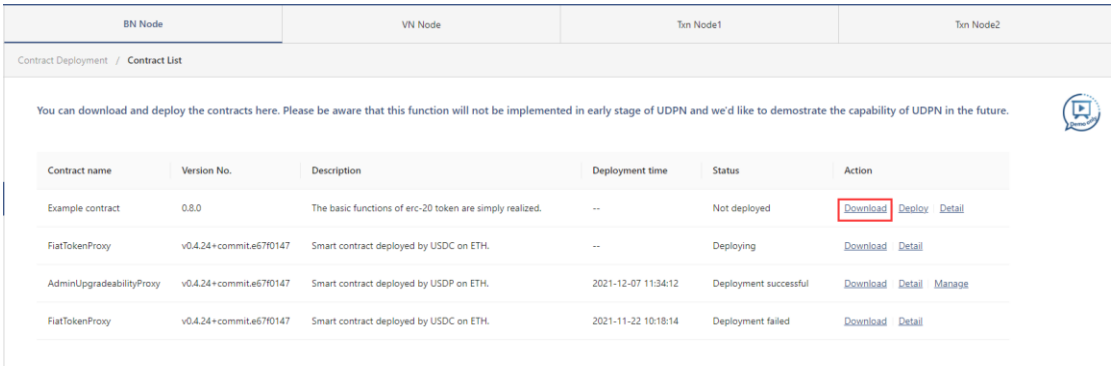


8. Contract Management

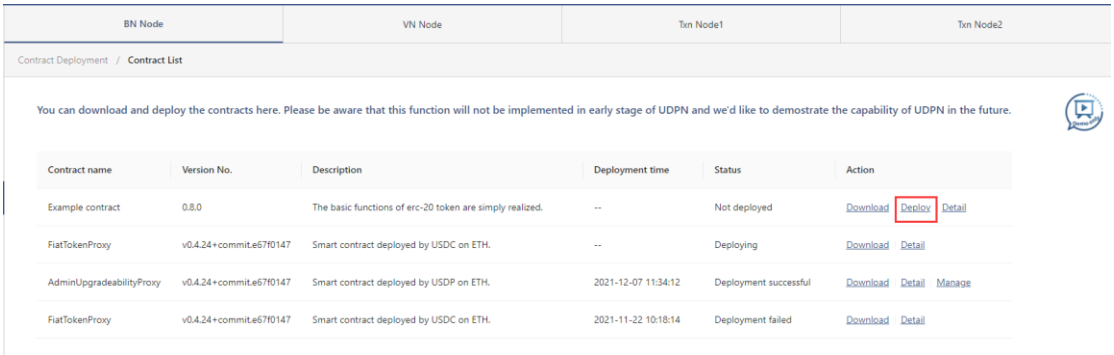
The sandbox provides sample smart contracts that users can download and review. Users can simulate the deployment of a smart contract in UDPN, review the call permissions, and access mock deployment information.

Smart contract management is for demonstration purposes only and has not been made operational yet. The smart contract management functionality will be available later in production.

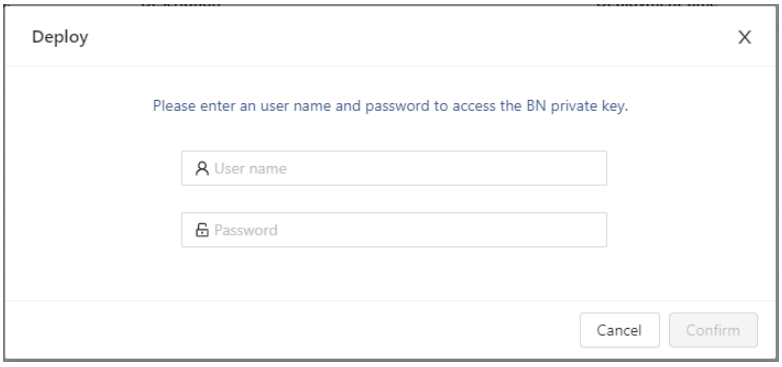
- **How to download a smart contract**: Choose one of the sample smart contracts from the list and click on the "Download" button to save the file locally.



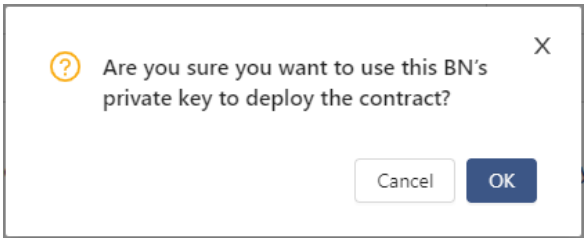
- **How to deploy a smart contract**: Choose one of the sample smart contracts from the list and click the "Deploy" button to simulate a smart contract deployment.



The private key for the Business Node is required to deploy a smart contract. You will be prompted to enter your username and password in the popup window first to access the Business Node private key.

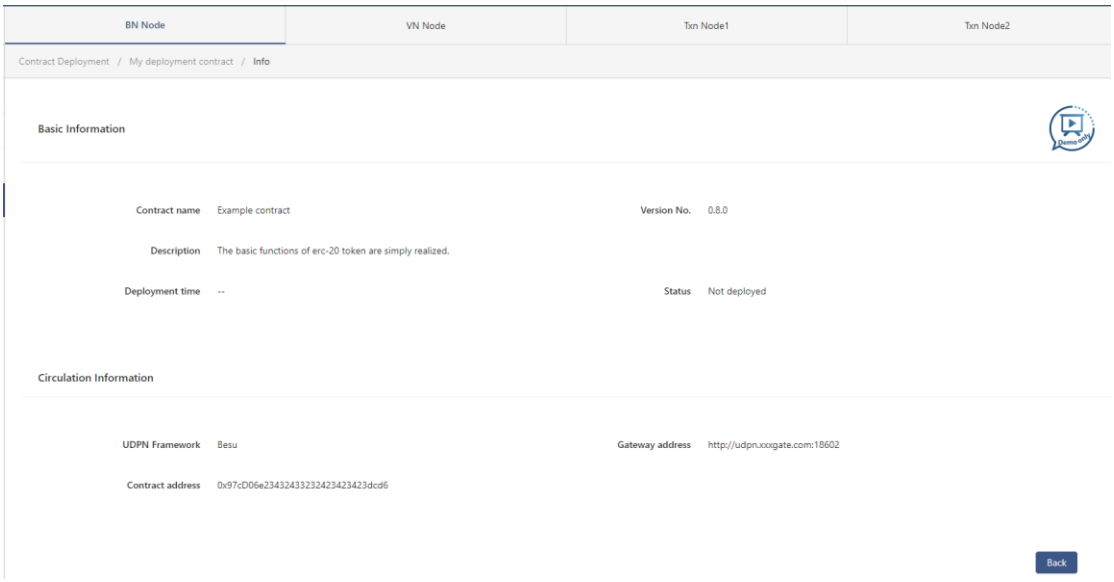


After entering the correct username and password, the system will prompt you to confirm that you want to use the Business Node's private key to deploy the smart contract. After clicking on the "OK" button, the smart contract deployment process starts.



- **Manage**: the "manage" link is used to manage contract permissions.
-

- **Detail:** The page below is used to check the deployment details following deployment.



9. Validator Node

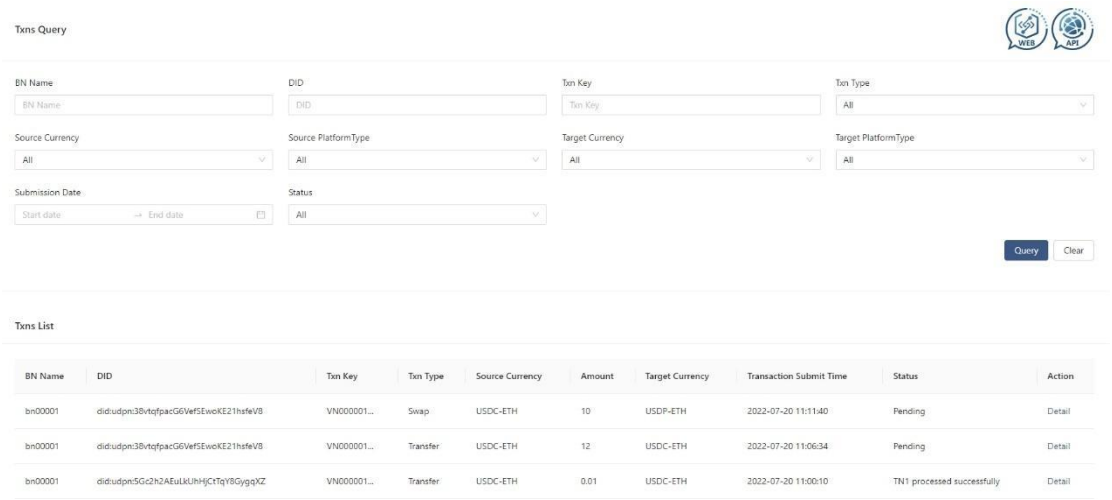
9.1 Overview

The Validator Nodes are at the heart of the UDPN, validating incoming message format and specific aspects of the content. VNs store the complete set of transaction data on the UDPN.

The Validator Nodes are connected to the Business and Transaction Nodes through secure APIs. The VN module in the UDPN Sandbox shows the transactions submitted by all business nodes.

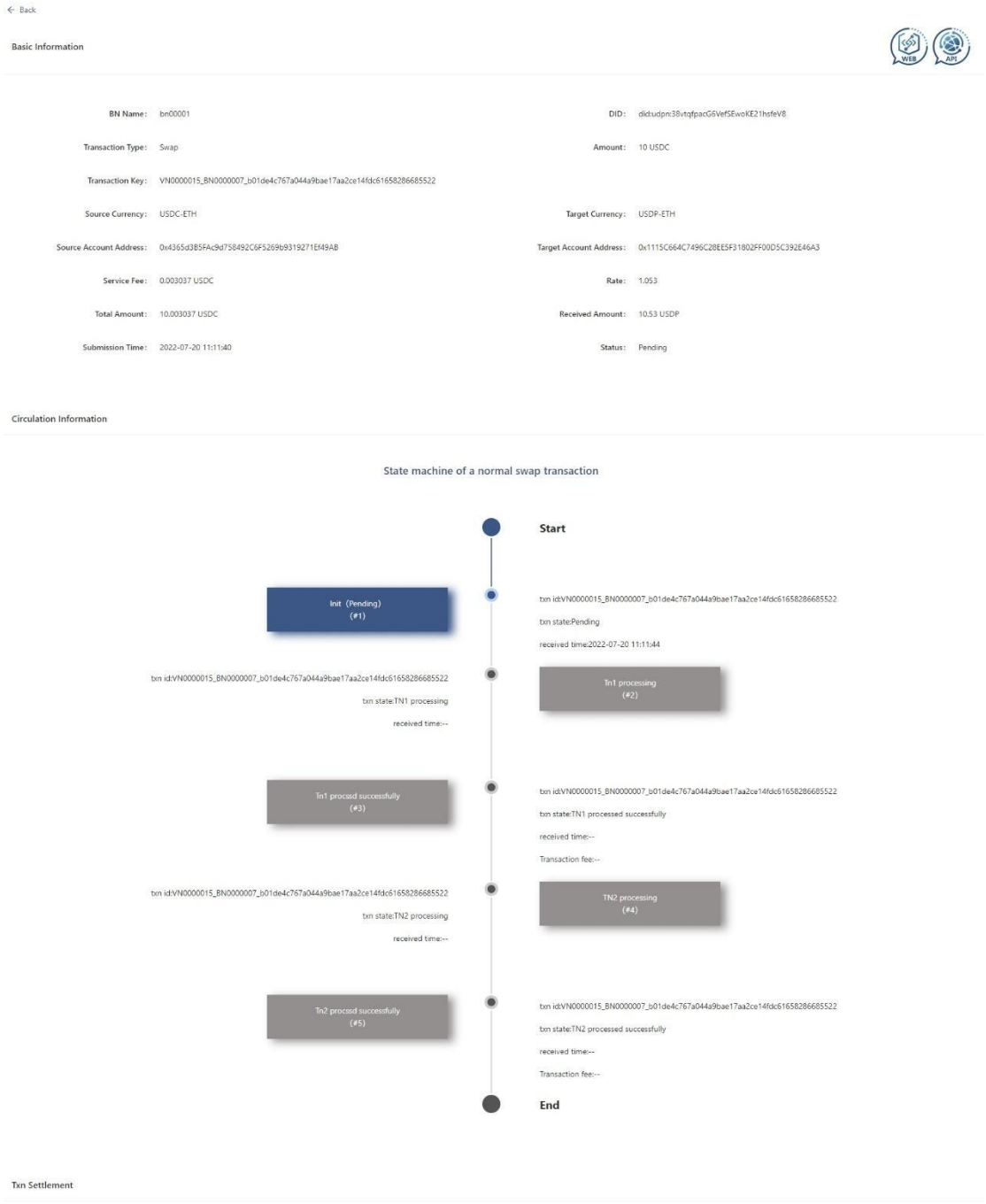
9.2 Transaction Query

You can query transactions by selecting the following information: BN Name, Transaction Type, Source Currency, Target Currency, Transaction Submission Date, Status, DID, Transaction Key. Then, click the "Query" button.



9.3 Transaction Details Display

This section displays transaction details, including DID, transfer, and settlement information.



10. Transaction Node 1

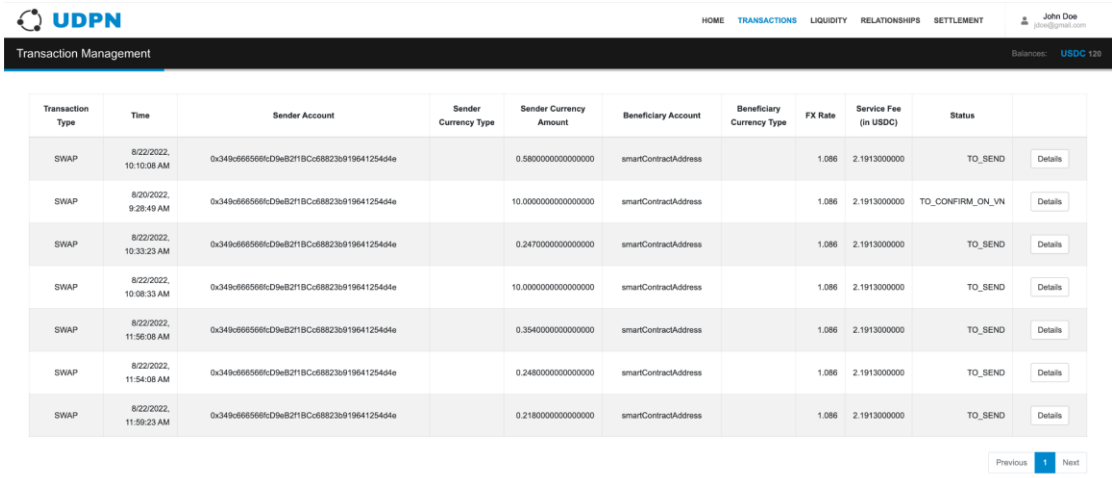
10.1 Overview

Transaction Node 1 is a mock Transaction Node (TN) deployed in the Sandbox environment. Each Transaction Node can only process one single currency on one currency system.

TNs are customized for each supported currency based on its respective currency system requirements (e.g., validation, transaction rules). Once a transaction initiated on UDPN is validated, it will be delivered and processed in the relevant digital currency system via a TN. The Sender needs to pay service fees for each transaction.

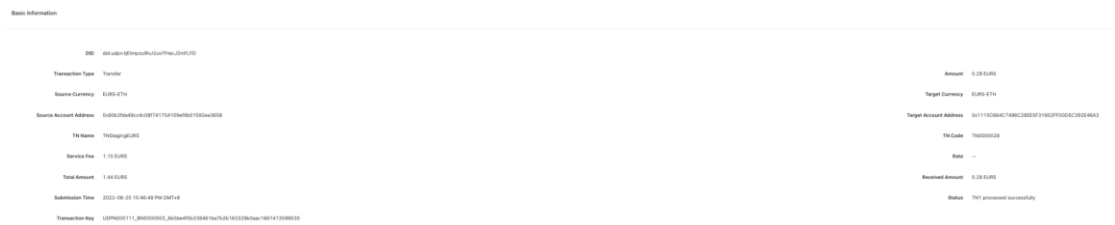
10.2 Transaction Query

Users can query transactions by selecting the following information: BN Name, Transaction Type, Source Currency, Target Currency, Transaction Submission Date, Status, DID and Transaction Key.



10.3 Transaction Details Display

The **Transaction Details Display** page summarizes transaction details, including DID, transfer, and settlement information.



State machine of a normal transfer transaction

11. Transaction Node 2

11.1 Overview

The Transaction Nodes supporting the Sender and Beneficiary currency must be selected before a swap. Each TN connects to a capital pool account supporting a single currency. In the first leg of the swap, the sender currency is transferred from the Sender's account to TN 1's capital pool. In the second leg of the swap, the Beneficiary currency is transferred from TN2's capital pool to the Beneficiary's wallet. The Sender must pay service fees for all transactions. Finally, TN 1 and 2 will regularly settle according to their agreed rulebooks.

11.2 Transaction Query

See section 9.2.

11.3 Transaction Details Display

See section 9.3