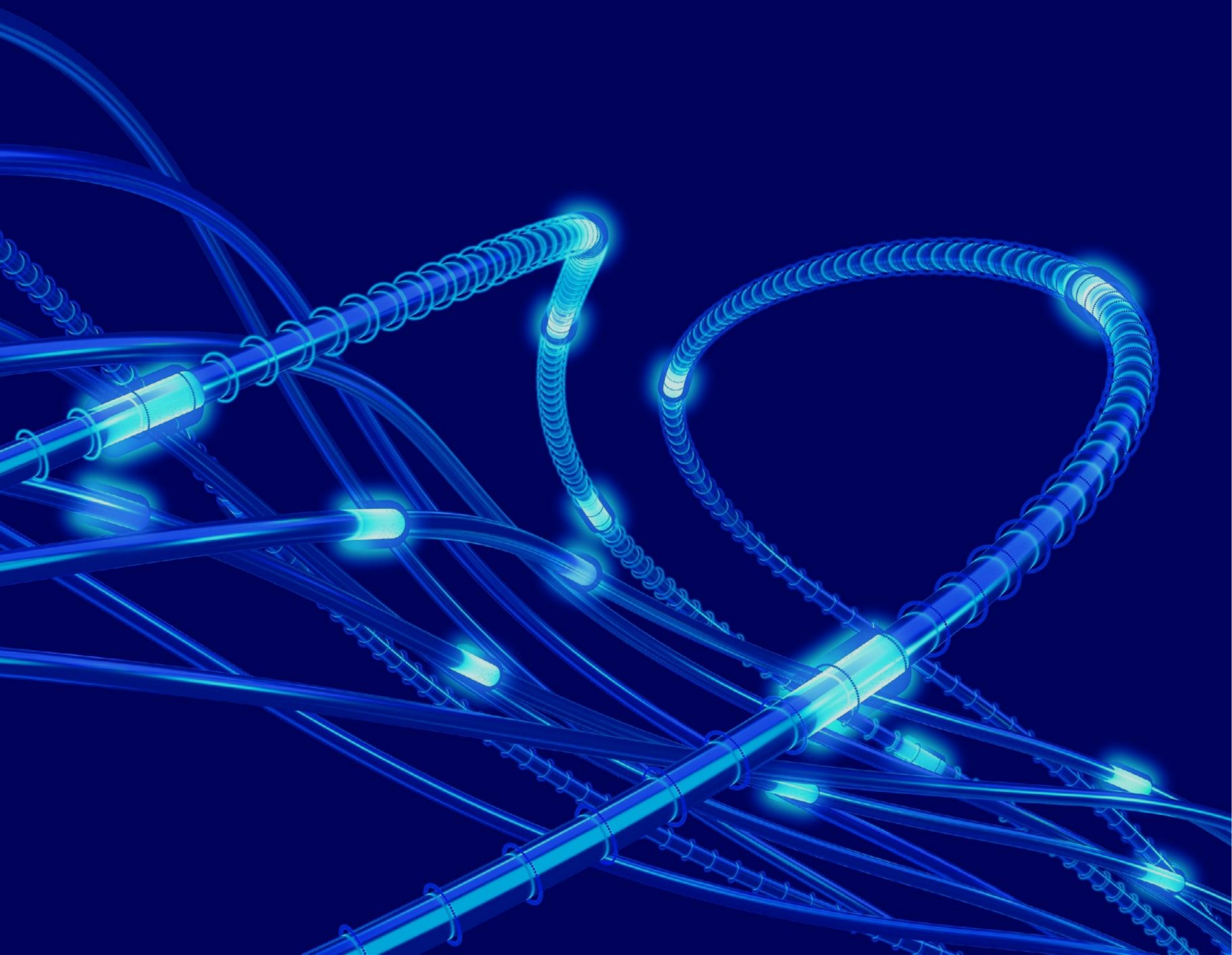
Universal Digital Payments Network

UDPN PoC Results: Transfers & Swaps on the Hedera Network

www.udpn.io



CONTENTS

Executive Summary

This Proof-of-Concept (PoC) pioneers the integration of high-performance public networks on the Universal Digital Payments Network (UDPN). Hedera is the first asynchronous BFT network supported by the UDPN. Thanks to its high transaction throughput, businesses can easily transact in digital currencies on the Hedera Network. Transactions are initiated on a UDPN Business Node, the gateway to all UDPN services, while integration complexities are abstracted by custom Transaction Nodes connected to the relevant Hedera digital currency systems.

This report presents the outcome of customising two Transaction Nodes to support digital currencies deployed on the Hedera Network. This PoC focused on integrating the Hedera Software Development Kit and EMTECH CBDC Sandbox, two leading digital currency frameworks, with the UDPN infrastructure. The primary goal was to validate the functionality of the UDPN network, enabling transfers and swaps of stablecoins and CBDCs on the Hedera testnet.

The HBAR Foundation and Swirlds Labs participated in this initiative, creating UDPN decentralised identities and linking them to their respective Hedera accounts. This report describes the PoC goals, achievements, design, and development process. In addition, it includes a cost analysis and comparison between Ethereum and Hedera as settlement layers and an analysis of Hedera technology as a UDPN messaging layer. Finally, we discuss security and privacy concerns related to digital currency transactions.

Copyright © 2024 UDPN. All rights reserved.

1. Introduction

The Universal Digital Payments Network (UDPN) is a leading blockchain infrastructure that facilitates transaction execution on multiple digital currency systems and powers interoperability at scale. This PoC demonstrates how the UDPN easily connects to high-performance public networks like Hedera.

The Hedera Network is an open-source, public, proof-of-stake network supporting high transaction throughput, predictable fees, and near-instant transaction finality. Compared to other open-source projects, Hedera concentrates on supporting real-world use cases and has designed its underlying technology to create one of the best developer experiences in the Web3 industry.

During the PoC, the HBAR Foundation and Swirlds Labs familiarised themselves with UDPN core concepts and services. GFT installed a Business Node for both entities. The Business Node is the gateway to all UDPN services. The UDPN infrastructure routes transaction messages from the Business Nodes to the Hedera Network. Customising the UDPN Transaction Node allows the creation of interoperable and programmable digital currency payment services across isolated settlement systems through a single gateway.

Copyright © 2024 UDPN. All rights reserved.

2. Architecture, PoC Core Components and Transactions

This section offers an overview of the Universal Digital Payments Architecture and the critical components demonstrated in this Proof of Concept. The core components are decentralised identities, stablecoins, CBDCs, and the UDPN User Acceptance Testing (UAT) environment.

2.1. Architecture Overview

The Universal Digital Payments Network (UDPN) is a blockchain-based infrastructure designed to foster the widespread adoption of digital currencies.

The UDPN is a non-custodial messaging network, meaning the users initiating the transactions control their digital currencies. The UDPN Alliance members, the entities operating the network, have no control over these assets. Businesses and financial institutions can initiate transactions on any digital currency system supported by the UDPN infrastructure (i.e., regulated fiat-backed stablecoins, tokenised deposits, and CBDCs). The UDPN infrastructure ensures all processed transactions are correctly signed and broadcasted to the right digital currency systems.

The network comprises four nodes, each vital in the transaction lifecycle. Two of these nodes are on-chain, while the other two are off-chain:

1. The Business Node (off-chain) is a gateway that connects businesses' IT systems to the UDPN services and allows businesses to initiate transactions.
2. The Validator Node (on-chain) is at the heart of the UDPN and validates the transaction requests from the Business Nodes.
3. The Transaction Node (off-chain) bridges the UDPN permissioned blockchain and digital currency systems. It broadcasts signed transactions.
4. The Transaction Audit and Reporting Node (on-chain) is a read-only archive node that allows auditors and regulators to monitor transactions for audit and compliance purposes.

Copyright © 2024 UDPN. All rights reserved.

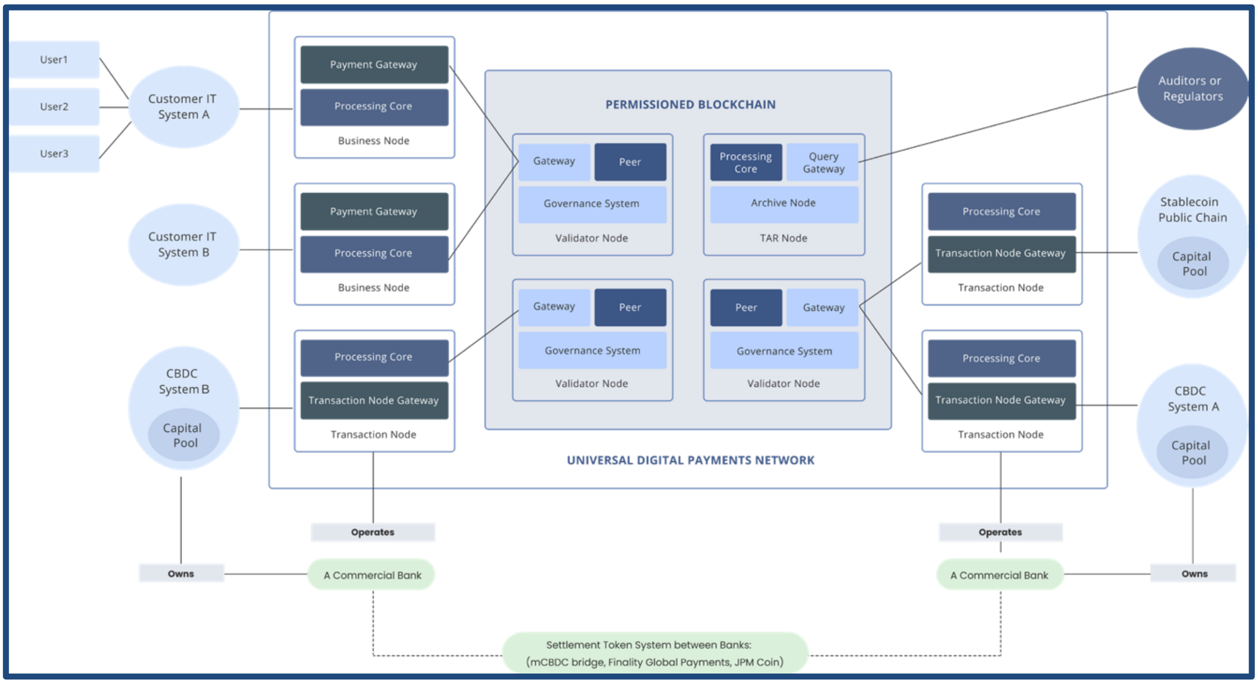


Figure 1: High-Level UDPN Architecture Overview

These four nodes compose the UDPN core infrastructure layer. Applications can be developed on top of this infrastructure. The Application layer supports two kinds of applications: the UDPN official services and third-party applications. UDPN official services include registering a UDPN decentralised identity (DID), mapping that DID to a digital currency address (e.g., a Hedera account), and initiating transfers/swaps. Third-party applications such as foreign exchange and cross-border remittances, Travel Rule compliance, etc., can be deployed by any authorised entity via a UDPN Business Node. Upon successful voting by the UDPN Alliance members, these applications will be available to other UDPN ecosystem stakeholders in an environment similar to an App Store.

2.2. Digital Currency Systems

This PoC focused on supporting end-to-end transactions on two digital currency systems: regulated fiat-backed stablecoins and central bank digital currencies deployed on the Hedera Network. In the following paragraphs, we define and describe each digital currency system.

Copyright © 2024 UDPN. All rights reserved.

2.2.1. Hedera Stablecoin Studio

The Hedera Stablecoin Studio is a new open-source SDK released by the HBAR Foundation, Hedera, Swirld Labs, and Iobuilders. This SDK simplifies developing and deploying stablecoin applications on the Hedera Network. The toolkit offers critical services such as a Proof-of-Reserve feature and custody provider integrations to strengthen trust and security. Stablecoins built with Hedera Stablecoin Studio support KYC/AML flags and related services to reduce the compliance burden on stablecoin issuers.

Below is a summary of the stablecoin we deployed with the Hedera Stablecoin Studio on the testnet:

Field	Value
EVM Address	0x00000000000000000000000000000000004311d3
Token ID	0.0.4395475
Name	USD_GFT
Symbol	USDGFT
Decimals	6
Initial Supply	1,000,100,000,000
Total Supply	1,000,100,000,000
Max Supply	Infinite
Treasury	SMART CONTRACT - 0.0.4395474

Table 1: Testnet Hedera Stablecoin Information

Since the stablecoin was deployed on testnet, we have deployed a simplified smart contract version and can integrate more advanced versions in production. Additional information on this token can be found via the following explorer link: https://hashscan.io/testnet/token/0.0.3980261

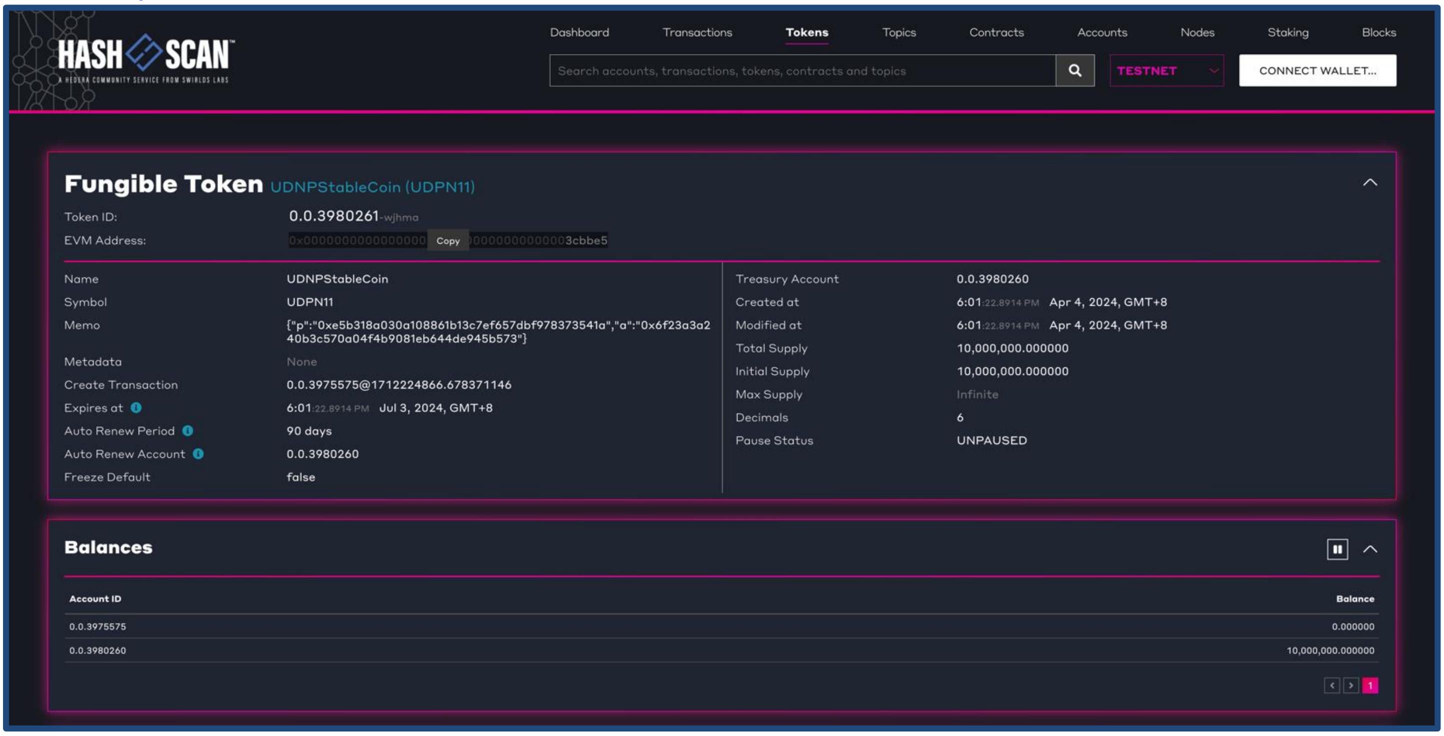


Figure 2: Testnet Hedera Stablecoin info on Hash Scan

Copyright © 2024 UDPN. All rights reserved.

2.2.2. EMTECH CBDC Sandbox

EMTECH is a leading CBDC technology provider that leverages the Hedera Network to issue and manage CBDCs. The company's certifications (ISO 27001 & SOC 2) testify to its professionalism, state-of-the-art cybersecurity, and compliance processes. EMTECH offers solutions catered to central banks and financial institutions. During this PoC, we leveraged the EMTECH Digital Cash Sandbox, which allowed us to use test CBDC tokens issued by the EMTECH Team. We customised the Transaction Node to support settlement via the Digital Cash Sandbox APIs and facilitate transaction message flows.

Field	Value
EVM Address	0x000000000000000000000000000000000014945d
Token ID	0.0.1348701
Name	Beyond Cash
Symbol	BYDC
Decimals	2
Initial Supply	60,000.00
Total Supply	60,000.00
Max Supply	Infinite
Treasury	0.0.5081351

Table 2: EMTECH CBDC Sandbox Information

Beyond Cash token is a simulated CBDC deployed on the Hedera mainnet, the details are available online via the following link:
https://hashscan.io/mainnet/token/0.0.1348701

2.3. Solution Overview

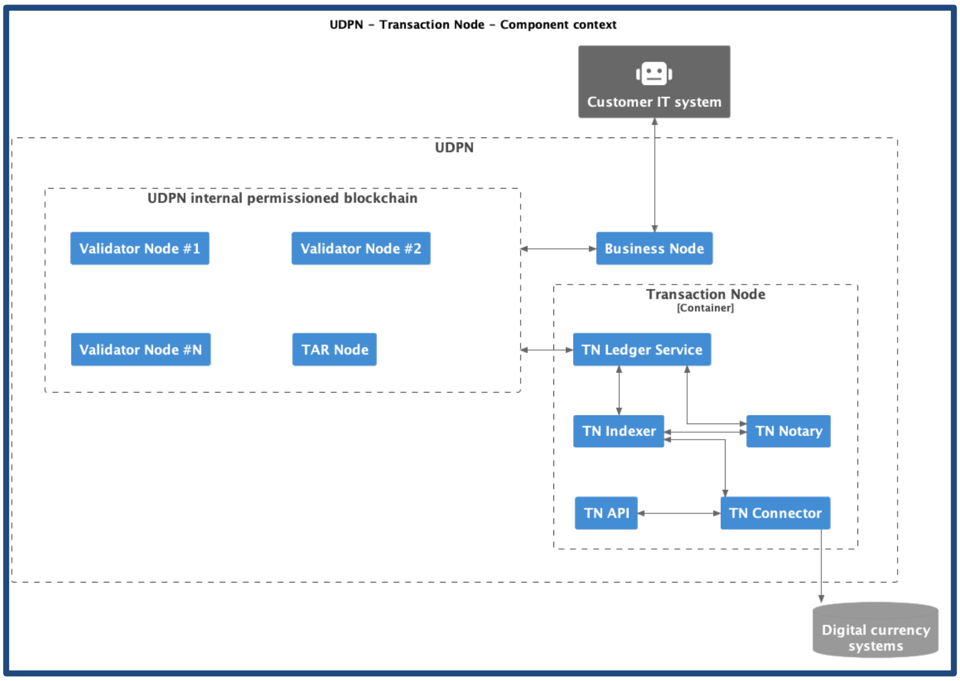


Figure 3: Transaction Node Architecture and Integration with UDPN

Copyright © 2024 UDPN. All rights reserved.

The UDPN orchestrates transaction requests, specifically transfers and swaps between digital currencies deployed on Hedera for this PoC. The UDPN infrastructure communicates the transaction messages to the Hedera Network via custom Transaction Nodes (directly using Hedera SDK and using EMTECH CBDC Simulator API)

The Transaction Node is a backend application composed of five services:

- Connector: This component listens to and registers transactions from the Hedera Network and acts as an interface for other services inside the Transaction Node.
- Ledger Service: This component is the heart of the Transaction Node. It acts as a local registry for UDPN transaction requests and an orchestrator that updates the status of UDPN transactions.
- Indexer: This component saves transactions from digital currency systems.
- Signatory: This component ensures that all data collected from external sources (i.e., external to the UDPN Validator Nodes) is not tempered.
- API services: These services allow a technical user or an application to make REST API calls to interact with and review transaction data processed by the Transaction Node.

The UDPN infrastructure was created to facilitate integration with various blockchain and digital asset platforms. The UDPN Transaction Node API specifies a set of interfaces that need to be implemented within a custom Transaction Node Connector that supports a specific settlement platform. Java was chosen as the technology for the Transaction Node API, making the Hedera SDK a natural fit.

This PoC focused on creating two instances of the Transaction Node, leveraging the Hedera Java SDK to broadcast stablecoin transactions on the Hedera testnet and the EMTECH Digital Cash Sandbox to broadcast test CBDC transactions on the Hedera mainnet. As part of this PoC, GFT implemented the Transaction Node components using the UDPN Transaction Node API.

To execute the transfer request built by the Business Node operators, the Transaction Node connected to the Hedera Stablecoin was modified to support the following functions:

- addTokenTransfer (<tokenId>, <accountId>, <value>): a method to specify the originator and beneficiary of the transaction, the transaction amount, and the token involved in the transaction
- freeze() along with setNodeAccountId() and setTransactionId(): a method to create an unsigned transaction before signing it
- sign(<private key>): a method to sign a transaction with a private key (ED25519)
- execute (client): a method to submit the transaction to the Hedera network
- getReceipt(client): a method to request the receipt of the transaction

Copyright © 2024 UDPN. All rights reserved.

- receipt.status: a method to collect the transaction status

These code modifications allow the UDPN participants to access payments on the Hedera Network seamlessly as the Business Node simplifies the integration process for potential new users. As a result, we expect additional use of Hedera Services for payments and higher transaction volumes on the Hedera Network. This work lays the foundation for additional integrations with other UDPN-branded solutions, such as the UDPN Tokenised Deposit and Stablecoin Management System.

Upon successfully adapting the Transaction Node code, we followed the following process to deploy the Transaction Node in the UDPN UAT Environment:

1. GFT configured the Transaction Node and performed a final code review.
2. Red Date set up a cloud instance for GFT to deploy the Transaction Node application in this cloud instance.
3. GFT worked closely with Red Date to deploy the Transaction Node in the pre-production environment and ensure it was properly onboarded.
4. GFT conducted test transactions to ensure the integration was indeed successful.

2.4. Decentralised Identity (DID) and Digital Currency Accounts

A UDPN DID is a unique identifier held by each user of the UDPN network services. Businesses can create a unique DID for each user or utilise a single DID for multiple users. Any entity can create UDPN DIDs by downloading the open-source Business Node software and our DID software development kit (SDK). By running the SDK locally, the business can create three essential documents: a document containing authenticating information, a document storing the corresponding private and recovery keys, and a document storing the DID string.

Digital currency accounts employed in this PoC were pre-funded with stablecoins and Hedera Test Tokens to cover gas fees. The table below illustrates the UDPN DIDs and digital accounts on the Hedera Network:

	Hedera Network Testnet
Sender DID	did:udpn:5aNRGN5Rn6Ge5gE9qLo46rktaYS
Source Currency Type/Digital Currency System	USDGFT-Hedera (a simulated stablecoin on testnet)
Account	0.0.4457106

Table 3: Test DIDs and Digital Currency Accounts

Copyright © 2024 UDPN. All rights reserved.

2.5. UAT Environment

GFT and Red Date deployed a UDPN Business Node in a UAT environment so that the HBAR Foundation could test the UDPN core functionalities via a dedicated UI. This UAT is hosted and will be maintained by Red Date for the entire duration of the PoC.

The testing environment caters to business and technical stakeholders with intuitive user interfaces and extensive API documentation. It allows its users to understand how multiple digital currencies can be used in various use cases. Commercial Banks, central banks, and potential alliance members can experiment with the four core UDPN transactions: creating decentralised identities, mapping them to digital currency accounts, performing currency transfers between accounts, and executing digital currency swaps.

During this PoC, the UDPN builders created a new set of Transaction Nodes supporting the Hedera Network technology stack and tested these in the UDPN UAT environment.

2.6. Transfer and Swap Processes and Sequence Diagrams

A UDPN transfer is a transaction between two parties within a single digital currency system, such as a USDC transaction between Alice and Bob on the Hedera Network. In this process, a specific amount of a single digital currency is moved from one account to another. The sequence diagram below describes a transfer flow on the UDPN.

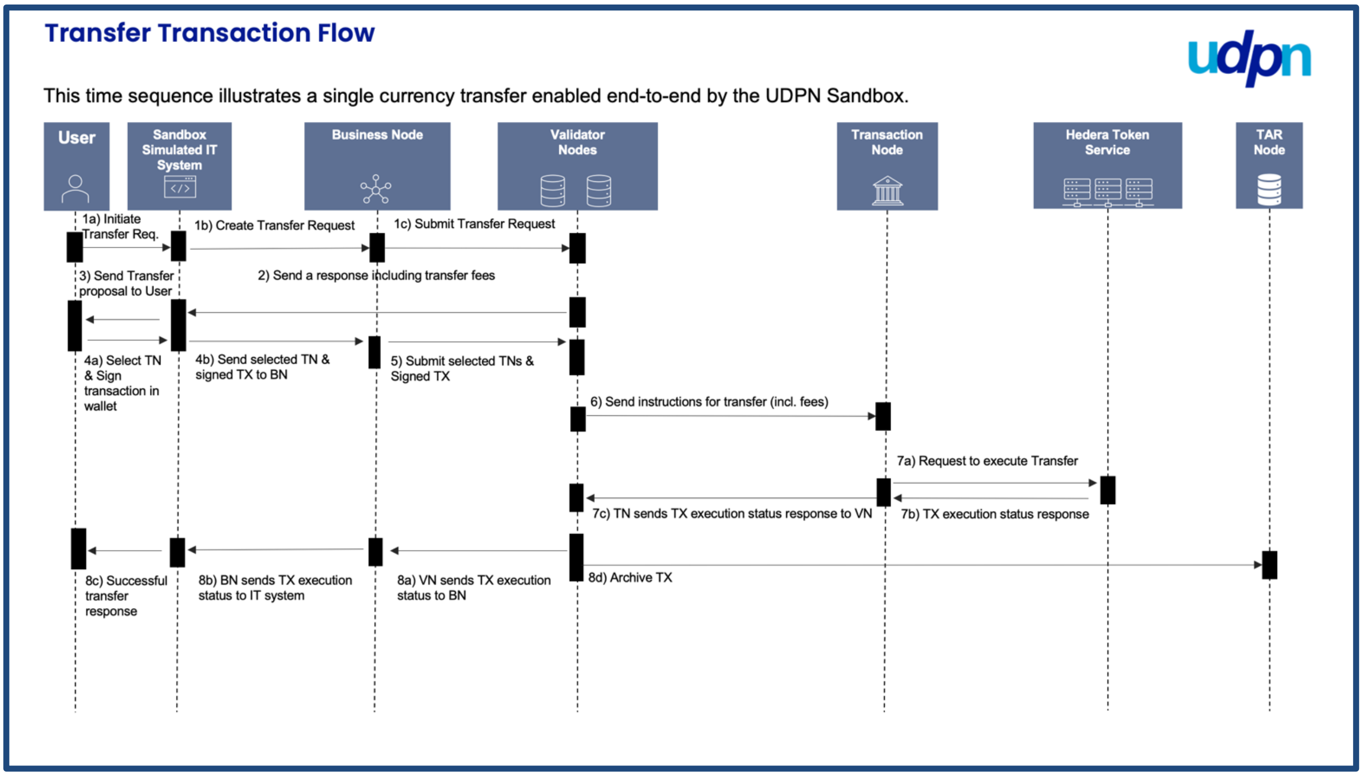


Figure 4: Transfer Sequence Diagram

Here is a detailed explanation of the transfer process for people not familiar with

Copyright © 2024 UDPN. All rights reserved.

UDPN transfers:

1. The user initiates the transfer via a web application by selecting their digital currency account and the digital currency they want to transfer. They also enter the amount of digital currency to be transferred and the beneficiary's digital currency account. Once all information is properly entered into the user interface, the application communicates this information to the Business Node via an API call. The UDPN Business Node also transfers the transfer request to a Validator Node via an API call.
2. The Validator Node receives the transfer request, validates the transfer information, and returns a set of Transaction Nodes supporting the digital currency entered by the user to the Business Node via an API call. The Business Node returns this information to the web application.
3. The user is presented with the list of Transaction Nodes that can broadcast the transfer transaction on their behalf.
4. The user selects the Transaction Node they trust to broadcast their transaction and sign the transactions to be broadcasted. Next, the web application transfers the Transaction Node information and the signed transaction to the Business Node via a dedicated API.
5. The Business Node submits the information about the selected Transaction Node and the signed transaction to the Validator Node, which once again validates the transaction format and calls a smart contract to orchestrate it.
6. The Validator Node sends the signed transaction and relevant instructions (e.g. transaction processing fees) to the Transaction Node.
7. The Transaction Node broadcasts the signed transaction to the Hedera Network, calling the Hedera Token Service. Once the transaction is broadcasted, the Transaction Node requests a transaction receipt via the Hedera SDK to ensure its successful execution. Upon receiving this message, the Transaction Node confirms the transaction status with the Validator Node.
8. The Validator Node transfers the execution status information to the Business Node, which transfers it back to the web application and the end user.

Conversely, a UDPN swap involving two digital currencies, a stablecoin and a CBDC, is split into two distinct transfers. During a swap, the originator sends their digital currency (stablecoin) to a stablecoin liquidity pool, while a CBDC liquidity pool operator transfers an equivalent amount of CBDC to the beneficiary. This arrangement guarantees seamless currency exchange regardless of the jurisdiction or underlying infrastructure, as each currency remains within its respective digital currency system. The sequence diagram below describes a swap flow on the UDPN.

Copyright © 2024 UDPN. All rights reserved.

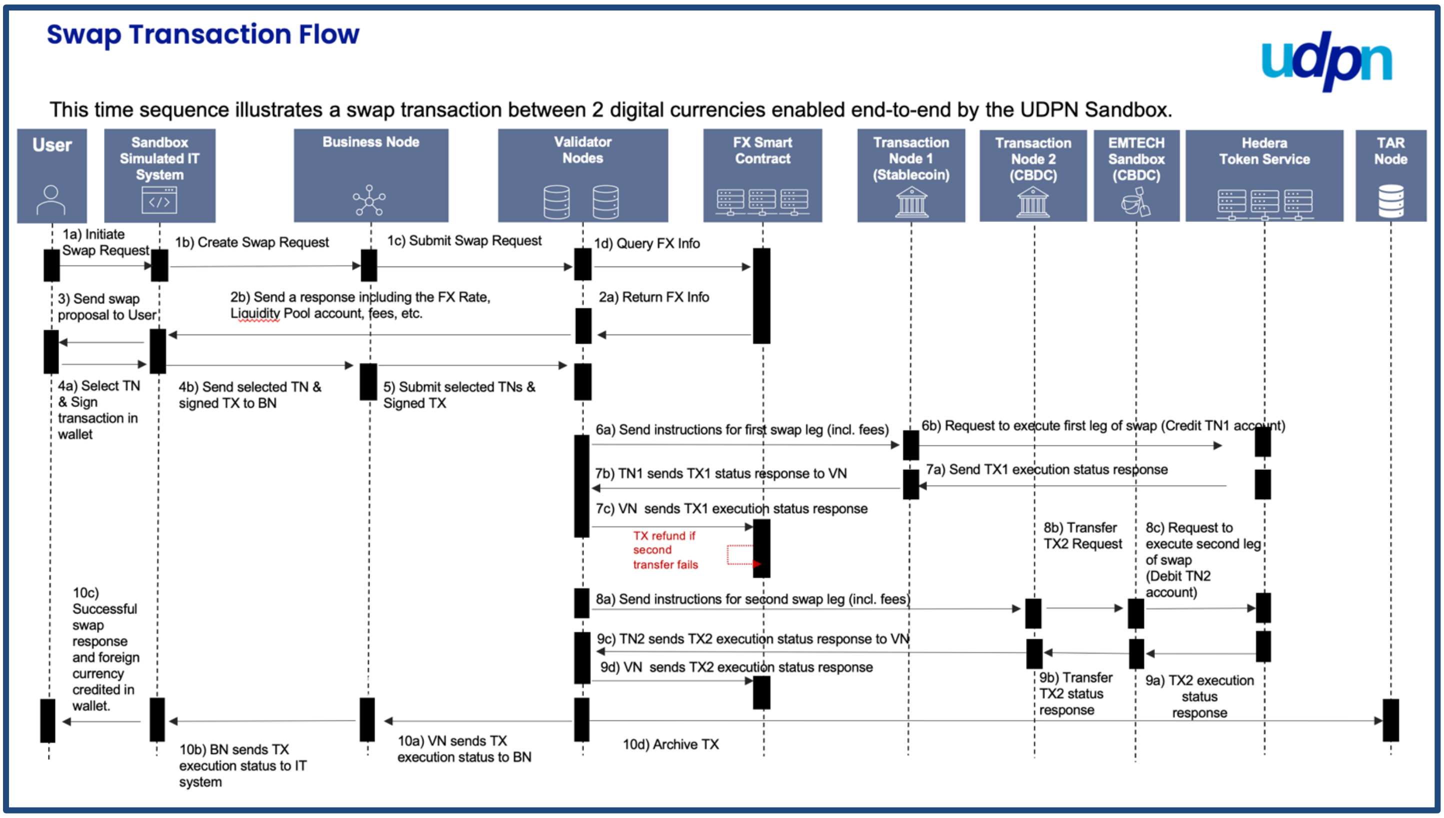


Figure 5: Swap Sequence Diagram

Here is a detailed explanation of the swap process:

1. The user initiates the swap via a web application by selecting their digital currency account, the symbol of the digital currency they want to transfer, and the symbol of the digital currency the beneficiary should receive. They also enter the amount of digital currency to be transferred and the beneficiary's digital currency account. Once the user validates the swap, the application communicates this information to the Business Node via an API call. The UDPN Business Node also transfers the swap request to a Validator Node via an API call.
2. The Validator Node receives the swap request, validates the swap information, and returns FX information with a set of Transaction Nodes supporting the digital currency swap requested by the user to the Business Node via an API call. The Business Node returns this information to the web application.
3. The user is presented with the list of Transaction Nodes that can broadcast the swap transaction on their behalf.
4. The user selects the set of Transaction Nodes they trust to broadcast their transaction and sign the transactions to be broadcasted. Next, the web application transfers the Transaction Node information and the signed transaction to the Business Node via a dedicated API.
5. The Business Node submits the information about the selected Transaction Nodes and the signed transaction to the Validator Node, which once again validates the transaction format and calls a smart contract to orchestrate the swap.
6. The Validator Node sends the signed transaction and relevant instructions (e.g., transaction processing fees) to the Transaction Node, which processes the first leg of the swap.
7. The Transaction Node processing the first leg of the swap broadcasts the signed

Copyright © 2024 UDPN. All rights reserved.

transaction to the Hedera Network, calling the Hedera Token Service. Once the transaction is broadcasted, the first Transaction Node requests a transaction receipt via the Hedera SDK to ensure its successful execution. Upon receiving this message, the Transaction Node confirms the transaction status with the Validator Node. The Validator Node confirms the first leg of the swap is successful by updating the UDPN FX smart contract.

8. The Validator Node triggers the second leg of the swap only if the first leg is successful. Upon confirming the first leg of the swap is successful at the previous step, the second leg of the swap is triggered, and relevant instructions (e.g., transaction processing fees) are sent to the Transaction Node, which processes the second leg of the swap. The Transaction Node signs a transaction, which ensures the digital currency entered by the transaction originator is delivered to its beneficiary.
9. The Transaction Node processing the second leg of the swap broadcasts the signed transaction to the EMTECH Sandbox, calling APIs built by EMTECH. Once the transaction is broadcasted, the second Transaction Node requests a transaction confirmation via the EMTECH Sandbox to ensure its successful execution. Upon receiving this message, the Transaction Node confirms the transaction status with the Validator Node. The Validator Node confirms the second leg of the swap is successful by updating the UDPN FX smart contract.
10. The Validator Node communicates the execution status information to the Business Node, which transfers it back to the web application and the end user.

Like Hedera, all UDPN swaps are atomic, meaning the beneficiary only receives their funds once the initial transfer from the originator to the first liquidity pool is successfully executed. If the second transfer from the liquidity pool to the beneficiary encounters any issues, the first liquidity pool ensures a full refund to the originator. This is achieved by the UDPN FX smart contract. Once the FX smart contract is aware that the second leg of the swap has failed, the smart contract triggers a refund transaction with the first Transaction Node. In such a case, the first transaction node signs a transaction and returns all funds to the swap originator.

2.7. PoC Transactions

During this PoC, the UDPN builders hosted a Business Node on behalf of the HBAR Foundation and provided associated credentials to allow the HBAR Foundation to complete test transactions in the UAT environment.

The HBAR Foundation created a decentralised identity, "did:udpn:5aNRGN5Rn6Ge5gE9qLo46rktaYS," and linked it to a dedicated digital currency account, "0.0.4457106".

Copyright © 2024 UDPN. All rights reserved.

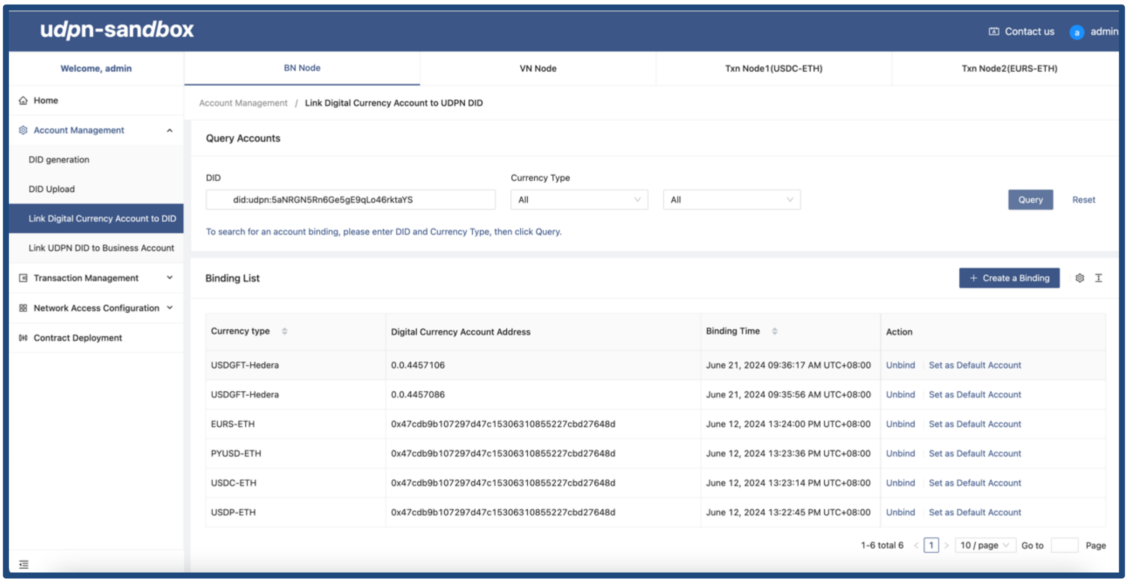


Figure 6: Link a Digital Currency Account with a DID

The HBAR Foundation team used a dedicated web application instead of making direct API calls for demonstration purposes. Upon accessing and logging into their account, they navigated to the "Transaction Management" tab and selected the "Transfer" sub-tab. Next, the HBAR Foundation Team filled in the details outlined in the table below:

Sender DID	did:udpn:5aNRGN5Rn6Ge5gE9qLo46rktaYS
Source Currency Type	USDGFT-Hedera
Send Account	0.0.4457106
Send Amount	1
Beneficiary Type	External Beneficiary
Beneficiary Account (Account associated with USDGFT-Hedera)	0.0.4457086

Table 4: HBAR Foundation Transfer Details

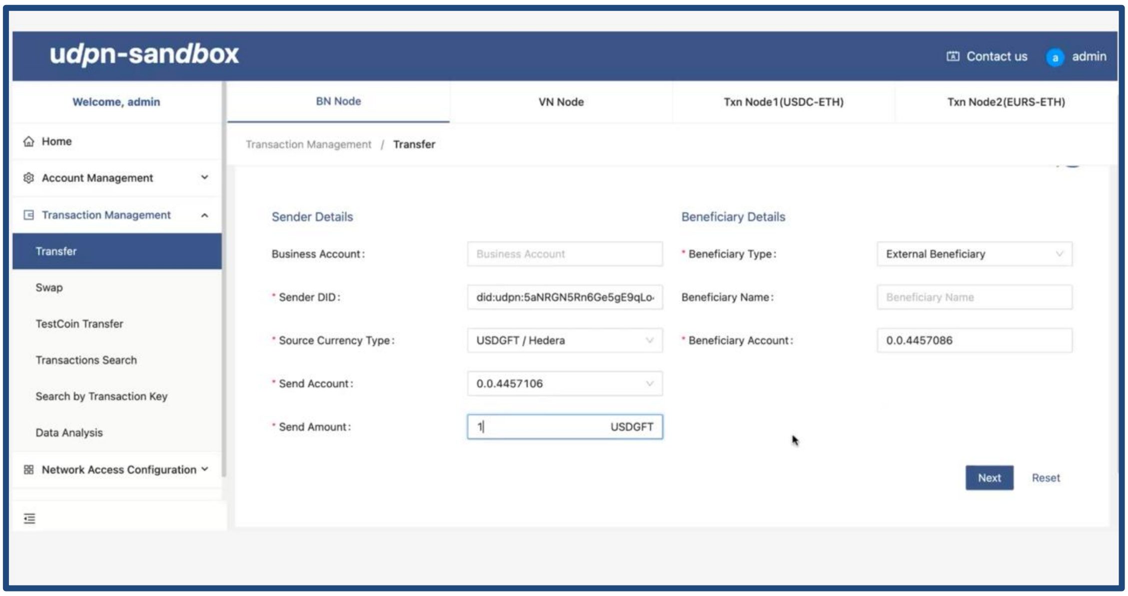


Figure 7: Transaction Management > Transfer

Copyright © 2024 UDPN. All rights reserved.

After entering the information above, they clicked on the action: "*Simulate Signing (end-user)*" and entered their private key.

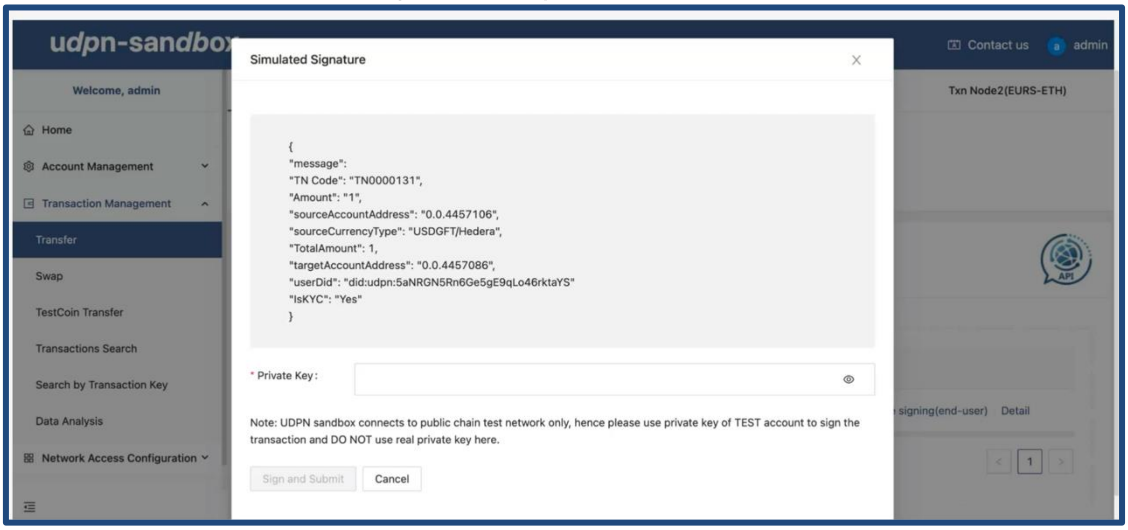


Figure 8: Simulated Signature

This triggered the transaction submission to the Validator Nodes and the team copied the following transaction key to track the transaction status: VN0000002_BN0000133_5977c58bb6fe4d5b829b029d902404901719906363451

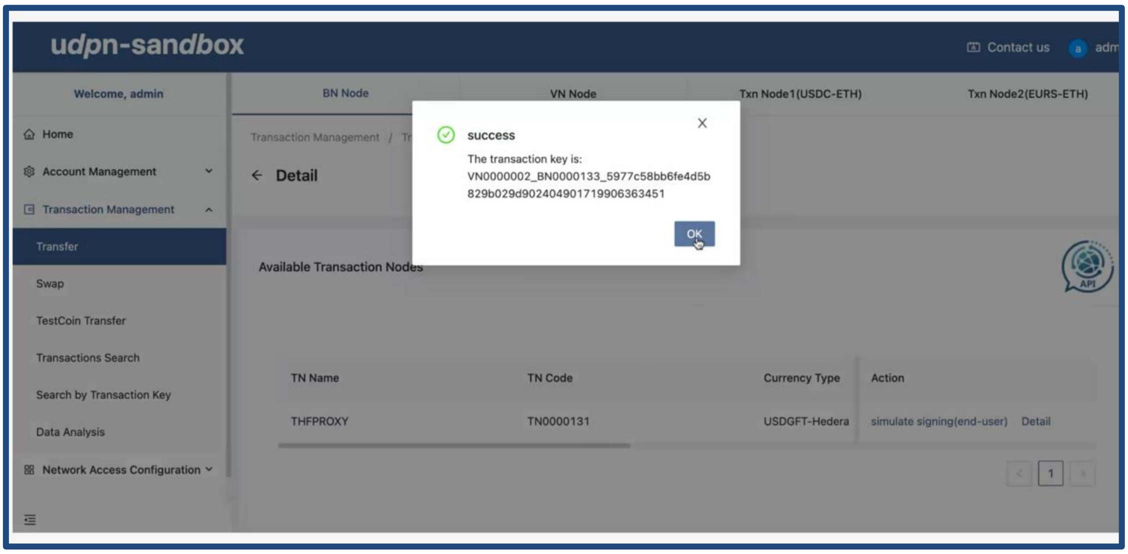
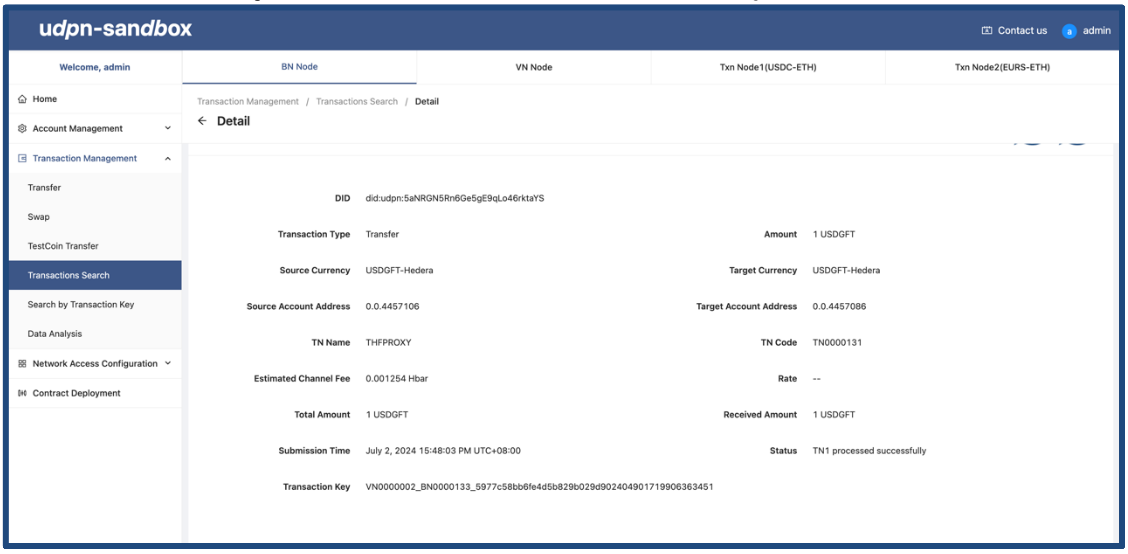


Figure 9: Transaction Key for tracking purposes



Copyright © 2024 UDPN. All rights reserved.

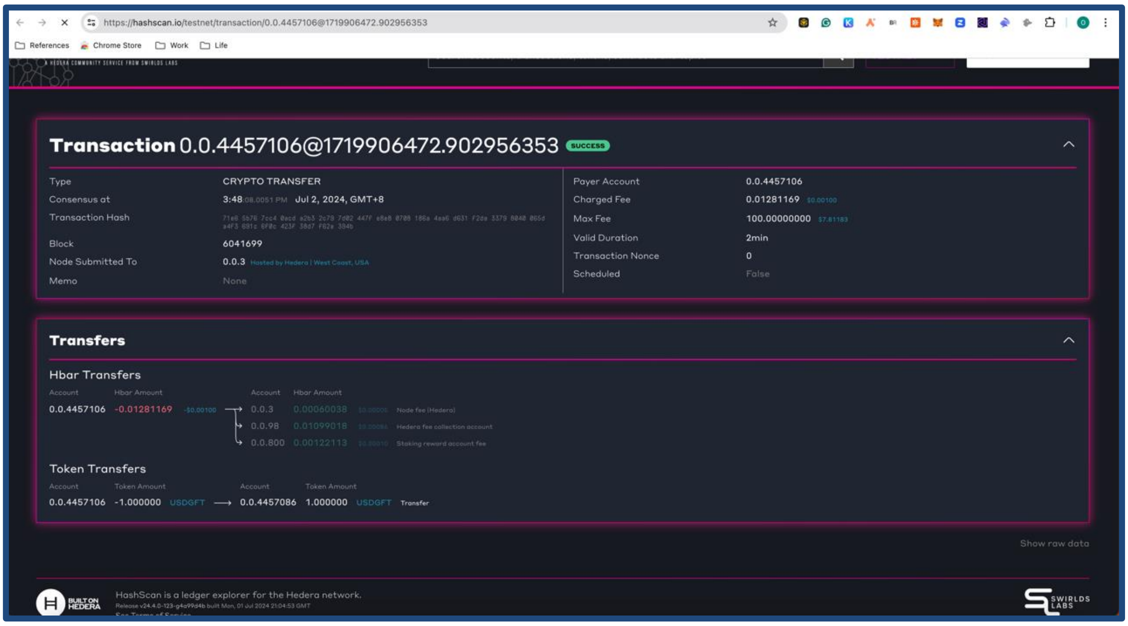


Figure 10: HBAR Foundation Transfer Information Summary (UDPN UAT & Hashscan Views) with test stablecoin

Note: Given the Hedera testnet resets every 3-6 months, this transaction may disappear from the explorer in the near future. For this reason, we included a screenshot of the explorer on the day of the transaction.

After confirming the transfer was successful, the HBAR Foundation team tested a swap between USDGFT-Hedera and PayPal USD (Sepolia Testnet version). The transaction details are presented below.

To complete the swap, the HBAR Foundation selected the "Swap" sub-tab under the “Transaction Management” Tab. Next, the HBAR Foundation Team filled in the details outlined in the table below:

Sender DID	did:udpn:5aNRGN5Rn6Ge5gE9qLo46rktaYS
Source Currency Type	USDGFT-Hedera
Destination Currency Type	PYUSD-Ethereum
Send Account	0.0.4457106
Send Amount	1
Beneficiary Type	External Beneficiary
Beneficiary Account (on Ethereum Sepolia Testnet)	0x902C51C16eA0654Bd0A2A63dfbD7d53a6eAE943C

Table 5: HBAR Foundation Swap Details

Copyright © 2024 UDPN. All rights reserved.

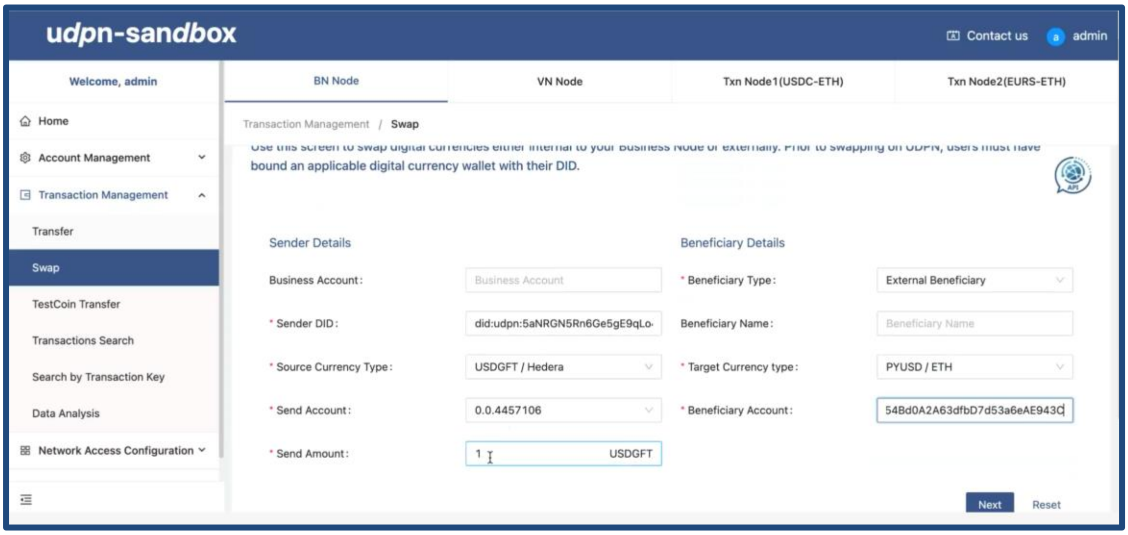


Figure 11: Transaction Management > Swap

After entering the information above, they clicked on the action: "*Simulate Signing (end-user)*" and entered their private key.

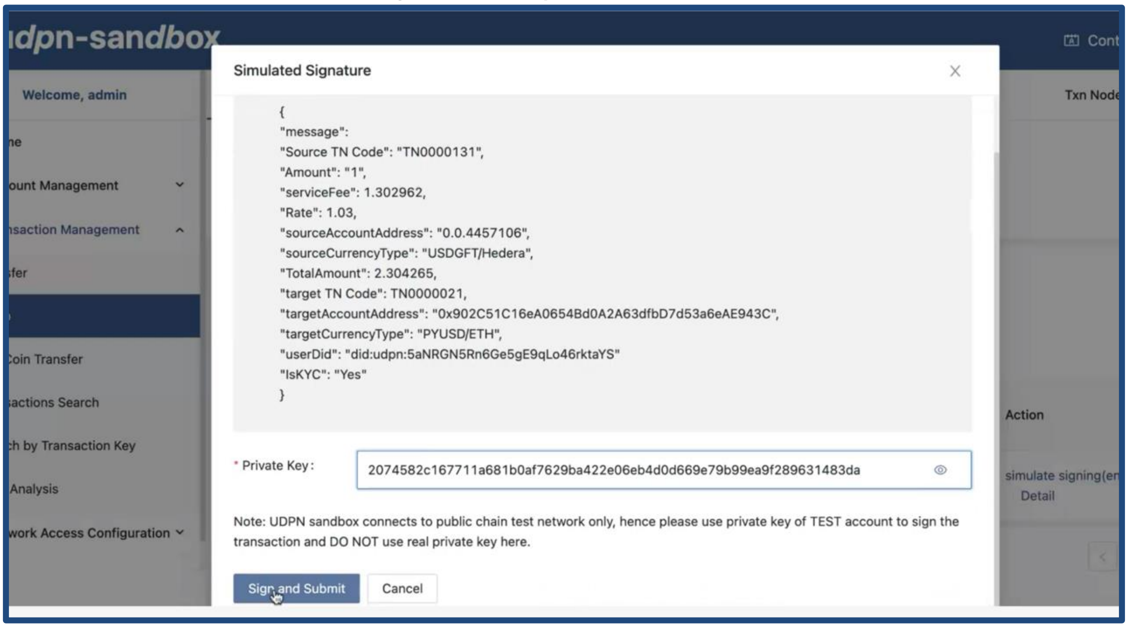


Figure 12: Simulated Signature

This triggered the transaction submission to the Validator Nodes and the team copied the following transaction key to track the transaction status: VN0000002_BN0000133_1a8148e149064744855524bcb16437512171990672 1457

Copyright © 2024 UDPN. All rights reserved.

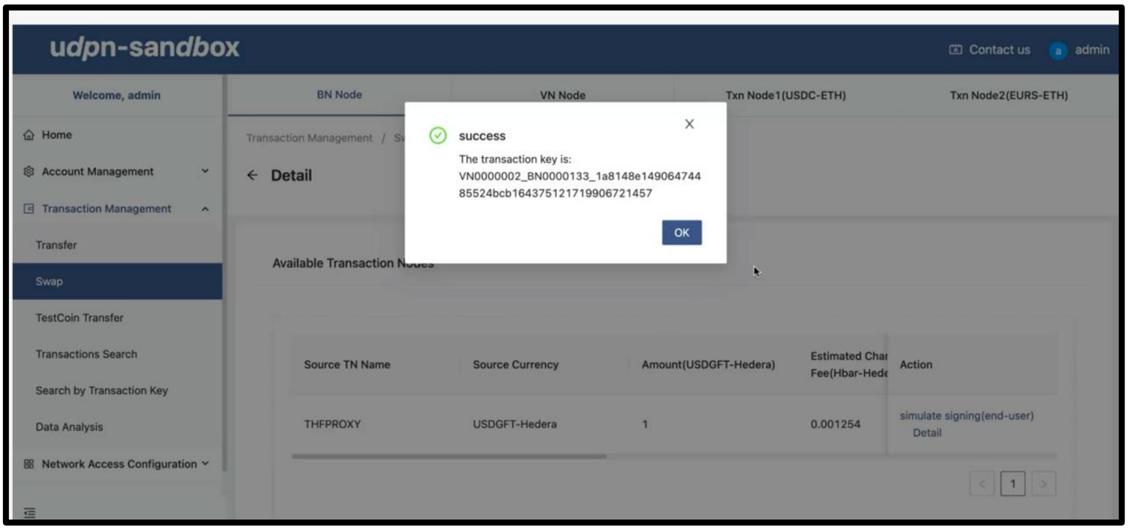
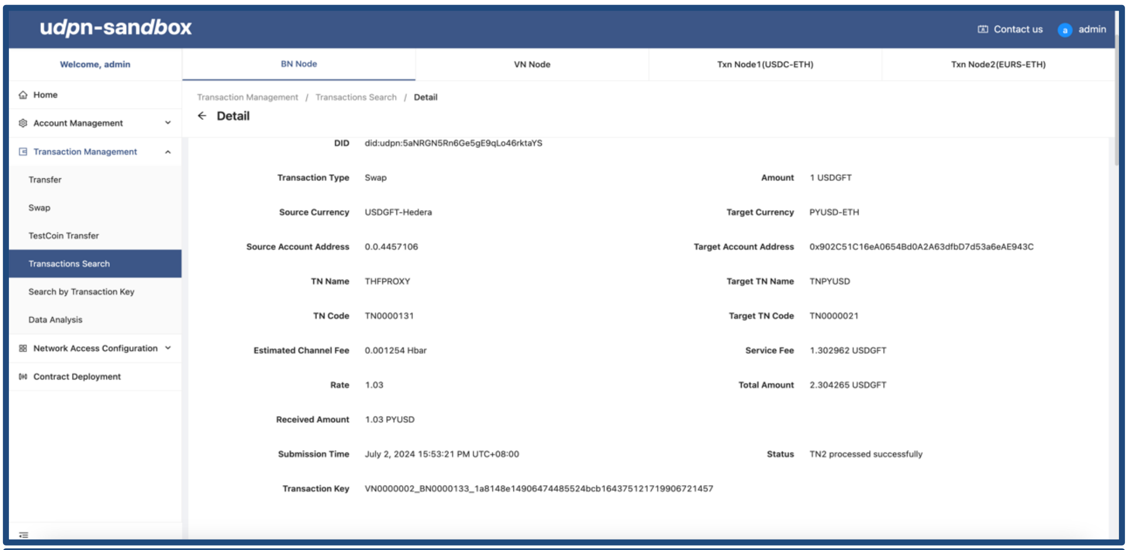
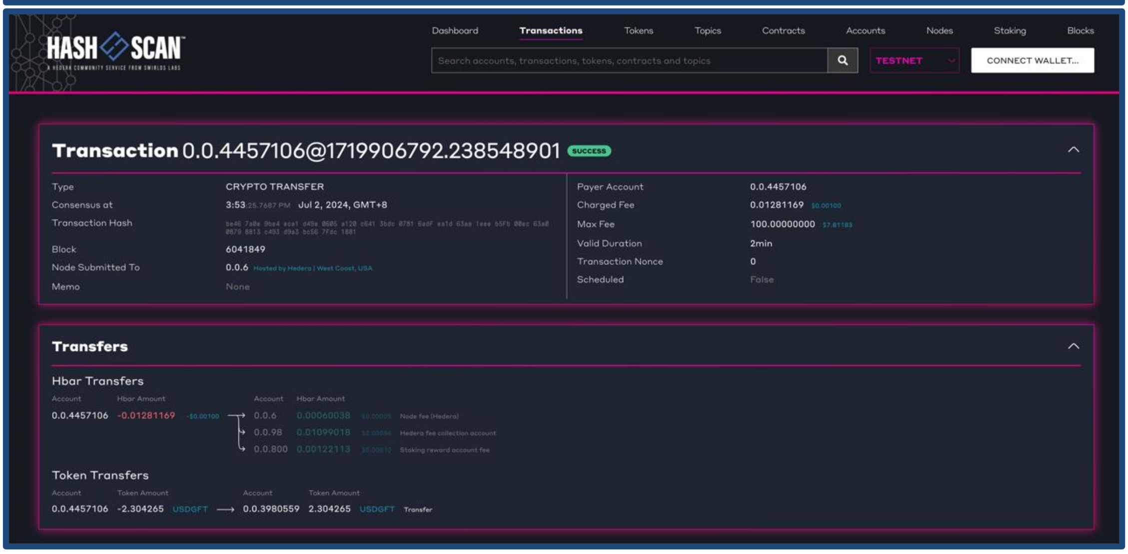


Figure 14: Transaction Key for tracking purposes





Copyright © 2024 UDPN. All rights reserved.

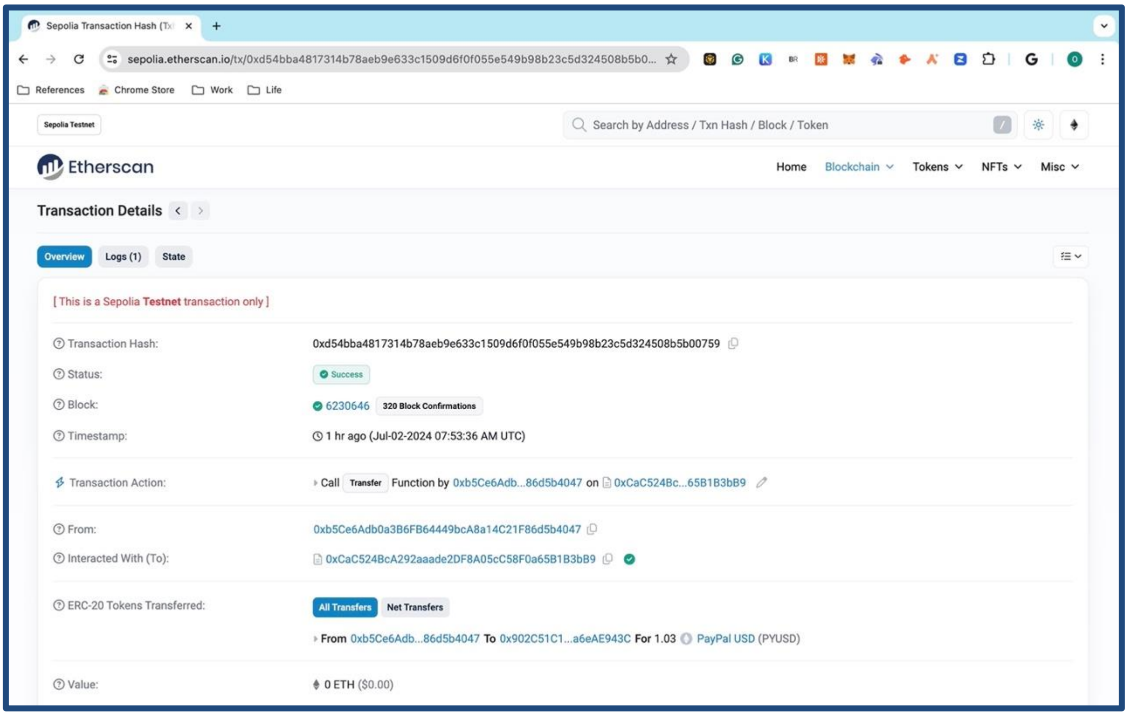


Figure 14: HBAR Foundation Swap Information Summary with test stablecoin (UDPN UAT, Hashscan, & Etherscan Sepolia Views)

Note: Given the Hedera testnet resets every 3-6 months, this transaction may disappear from the explorer in the near future. For this reason, we included a screenshot of the explorer on the day of the transaction.

In addition to testing transactions between, the HBAR Foundation also completed test transactions via a Transaction Node connected to the EMTECH Sandbox. The process was almost identical to the steps described for the stablecoin transfers and swaps. Therefore, we only present the transaction results below.

Figure 15: HBAR Foundation Transfer Information summary with test CBDC

Figure 16: HBAR Foundation Swap Information Summary with test CBDC

Copyright © 2024 UDPN. All rights reserved.

(UDPN UAT, Hashscan, & Etherscan Sepolia Views)

3. PoC Process

Since its inception in 2020, the UDPN team has devoted substantial efforts to helping financial institutions and partners understand the significance of the Universal Digital Payments Network, digital currencies, and our vision for the future of payments.

This section introduces the UDPN PoC Management Process and offers a non-exhaustive compilation of answers to questions stemming from this PoC. We compare the Hedera Network and the Ethereum Network as settlement layers. We also perform a functional analysis to determine whether the Hedera Network underlying technology could be used as one of the blockchains powering the UDPN messaging infrastructure. Finally, we clarify security and privacy concerns.

3.1. PoC Management Process

The UDPN Team has created a standardised management process for each PoC. This process allows the team to conduct multiple PoCs simultaneously in an organised and structured manner. In this PoC, GFT and Red Date Technology took on the PoC Project Manager and builder roles while the HBAR Foundation and Swirlds Labs were Observers. Each role is described in the figure below:

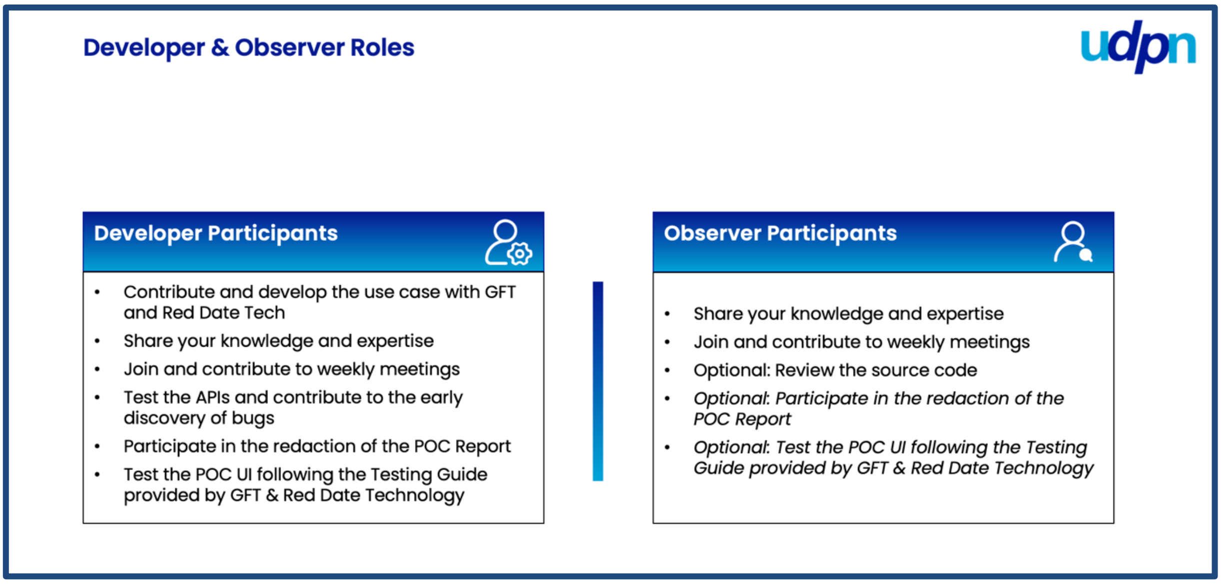


Figure 17: PoC Builder vs Observer Roles

The PoC started with a kick-off meeting on March 28th, 2024, to help all stakeholders (mainly GFT and the HBAR Foundation) align on the PoC objectives, timelines, and management procedures. Working methods and communication lines were established during the kick-off meeting to ensure smooth information sharing (primarily via Slack and email).

Copyright © 2024 UDPN. All rights reserved.

Given this PoC resulted from a grant application, the business requirements and technical design documents were already in place, which allowed GFT to start the development work right after the kick-off meeting.

All stakeholders met ad hoc to review progress and provide feedback on the PoC. After each meeting, all participants received a report, including a Status Summary and Action Logs. A RAG document was also created to keep track of risks and mitigations discussed during the project.

GFT demonstrated test transactions in digital currencies. The first demo focused on validating the stablecoin transfer functionality and a stablecoin swap from the Hedera Network to the Ethereum (testnet). The second demo focused on validating the CBDC transfer functionality and a CBDC-stablecoin swap from the EMTECH CBDC Sandbox to the Ethereum (testnet). GFT and Red Date also deployed a dedicated web application to allow ongoing testing by the HBAR Foundation.

This work culminated with the publication of this report.

3.2. Business Considerations

3.2.1. Comparison between the Hedera Network and Ethereum as settlement layers

Online payments are ubiquitous today. Consumers use instant payments for daily transactions, such as paying for a coffee with their phones or cards and online shopping. Yet, merchants must wait for days, if not weeks, to receive debit and credit card payments, making it difficult to manage cash flows. Cross-border transactions are another example of current payment inefficiencies. Blockchain technology has the potential to reduce settlement time dramatically, as already demonstrated by digital asset markets operating 24/7/365.

When comparing settlement alternatives, the following network features should be considered: transactions per second, average fees, transaction finality, and energy consumption. The primary use case for settlement layers is instant payments between individuals and businesses, supporting people's livelihoods. High throughput is required to support a significant number of transactions, powering entire economies at scale. Transaction finality ensures that payments cannot be easily reversed, providing economic security for the recipient. Fees must be reasonable and predictable to ensure everyone can access payment services and businesses can predict their costs accurately. Finally, energy consumption is increasingly important as countries aim to achieve their Net Zero Emissions Targets by 2030, and digital payment infrastructures operating 24/7 may lead to excessive energy consumption if not correctly designed.

The table below compares Ethereum (mainnet) and the Hedera Network based on the above metrics.

Copyright © 2024 UDPN. All rights reserved.

Metrics	Hedera Network	Ethereum Mainnet
Transactions per second	Up to 10,000	30
Average Fees	$0.0001	$0.94
Transaction Finality (Seconds to Consensus Finality)	3.48	10-20 seconds
Energy Consumption (Average WH/TX)	0.003	9.956

Table 6: Functional Comparison of the Hedera Network & Ethereum Mainnet

While layer 2s are playing an increasing role on the scaling roadmap of competing layer 1s, the Hedera Network is a superior alternative to most public layer 1s today. Hedera is considering sharding solutions to increase its transaction throughput. Furthermore, network fees are fixed, denominated in USD, and paid in $HBAR, allowing businesses and technology companies to predict their costs easily, contrary to most public blockchain protocols. Finally, the Hedera Network is an energy-efficient infrastructure with firm ESG commitments. While building a network that consumes the least energy amongst its peers, Hedera has purchased carbon offsets to become a carbon-negative infrastructure.

3.2.2. Institutional Adoption of the Hedera Network

The UDPN aims to become a global network with a broad geographical and sector representation. Similarly, the Hedera Council is governed by 32 organisations, including Google, Nomura, IBM, Deutsche Telekom, and EDF. The composition of the Council is striking as it is diverse and includes companies from different industries: information technology, legal services, custody, financial services, aviation, telecommunication, gaming, etc. These companies ensure the network's stability, timely upgrades, governance, and operations. While most public blockchains start as decentralised initiatives and lack proper due diligence on their validators, the HBAR Foundation has curated a group of diverse participants to ensure a gradual approach to decentralisation, fostering trust as the network becomes increasingly decentralised. This operating model is aligned with the UDPN 's operating model. We expect to continue exploring synergies with the HBAR Foundation and driving institutional adoption for both infrastructures.

In April 2024, the HBAR Foundation, Ownera, and Archax announced Blackrock's ICS US Treasury money market fund had been tokenised on Hedera. FCA-regulated digital asset exchange Archax launched a new set of tokenised shares after successfully listing tokenised shares of a multi-billion money market fund last year. This is a testament to regulated institutions' trust in the Hedera Network and its underlying technology. These are just two examples of the countless use cases the Foundation has spearheaded to encourage the use of its technology in real-world use cases, such as carbon credit tokenisation, tokenisation of loyalty programs, and real-time payments.

Copyright © 2024 UDPN. All rights reserved.

3.2.3. Hedera Integration with UDPN Solutions & Future Participation

During this PoC, the UDPN builders and the HBAR Foundation organised multiple training sessions to foster a greater understanding of our joint offerings and define further areas for collaboration. The HBAR Foundation introduced the Hedera Stablecoin Studio, an SDK that allowed us to speed up our development efforts. It provided regular technical support as the UDPN development team integrated Hedera currency systems with the Transaction Node. The Stablecoin Studio allowed us to issue our first test tokens on testnet within a day of starting the project without previously working on Hedera technologies.

The UDPN builders team introduced the UDPN All-in-One Digital Currency Sandbox, one of the world's most advanced digital currency sandboxes, and the Tokenised Deposits and Stablecoins Management System, the first production-ready solution offered by the UDPN builders.

In March 2024, the UDPN builders, GFT and Red Date Technology, launched the UDPN All-in-One Digital Currency Sandbox. It is the world's most powerful digital currency sandbox for commercial and central banks. The UDPN Sandbox serves multiple purposes.

The UDPN All-in-One Digital Currency Sandbox is an institutional-grade secure environment for deploying a multitude of innovative use cases and experimenting with programmable applications. The Business Node operators can easily deploy smart contracts run on the UDPN EVM. Application developers will be encouraged to build new services on top of the UDPN infrastructure and will benefit from the support of the UDPN Alliance members to build successful ventures.

After the user acceptance testing phase, the Transaction Nodes supporting the Hedera SDK and the EMTECH CBDC Sandbox might be made available to UDPN Sandbox clients as an add-on service.

All parties agreed to explore integrating the Hedera Network as an add-on to the UDPN All-in-one Sandbox. In addition, the HBAR Foundation expressed interest in integrating the Hedera Stablecoin Studio with the UDPN Stablecoin Management & Tokenised Deposits Management System.

3.3. Technical Considerations

3.3.1. Leveraging Hedera Technology on the UDPN

The UDPN is a decentralised messaging infrastructure that uses smart contracts to orchestrate transactions across multiple digital currency systems. With minimal changes, the UDPN smart contracts can be run on any permissioned EVM-compatible blockchain, including the Hedera technology stack.

Copyright © 2024 UDPN. All rights reserved.

Over the past few years, Hedera has ramped up its EVM support to appeal to Solidity developers and provide additional flexibility to its developer community. The Hedera EVM was built on top of a Hyperledger Besu EVM client, which would make deploying UDPN smart contracts seamless on a custom version of the Hedera infrastructure. Yet, this EVM implementation also includes optimisations specific to the Hedera technology stack.

Notable differences between Hedera and Ethereum exist:

- Both ECDSA and non-ECDSA accounts supported by Hedera are compatible with the Hedera EVM
- Contracts can expire, and a recurring payment (rent fees) may be required to ensure contacts remain active on the network. There are two kinds of rent fees: auto-renewal fees and storage costs.
- Hedera technologies do not require mempools to process incoming transactions because of the asynchronous byzantine fault-tolerant consensus algorithm described in Section 3.3.3.

During this PoC, the UDPN builders determined that additional integration work would also be required to support Hedera technologies at the Validator Node level. The Validator Nodes are the heart of the UDPN, connecting Business Nodes to Transaction Nodes. If the UDPN used the Hedera tech stack as one of its underlying technologies, the Validator Nodes would need to be mapped to a permissioned network of Hedera Consensus Nodes and run by the UDPN Alliance members.

3.3.2. Implementation differences between "traditional" EVM Transaction Nodes and Hedera-Compatible Transaction Nodes

One key difference between our "traditional" EVM Transaction Nodes and Hedera-compatible Transaction Nodes is that Hedera does not support transaction blocks, as all transaction information is stored in transaction record files on the Mirror Nodes. A mirror node is an archive node that stores transaction records, events files, and balance files. Besides the Mirror Node, it is also possible to query basic transaction information from a Consensus Node. The UDPN development team adapted the Transaction Node connector to collect transaction data via API calls to a Consensus Node.

In addition, during the integration work, GFT software engineers discovered gRPC compatibility issues because the Transaction Node used Maven plugin, which was incompatible with the light version of gRPC delivered with Hedera SDK. To remediate these issues, the team decided to use Gradle instead of Maven to build the Transaction Node implementation for the Hedera Network. At the same time, the team responsible for the Hedera SDK reported that they were ready to prepare a special release. This release would include a full gRPC library, ensuring that all future implementations, including Hedera SDK, should be seamless.

3.3.3. Hedera Network Security

Copyright © 2024 UDPN. All rights reserved.

Hedera's security is ensured by a robust and scalable consensus algorithm: an *asynchronous* byzantine fault-tolerant protocol. This algorithm guarantees the network will always reach consensus, contrary to other public blockchains. This unique approach allows Hedera to avoid using mempools, which create congestion issues and MEV (Maximum Extractable Value) attacks on public blockchains such as Ethereum. The Hashgraph consensus only assumes that at least two-thirds of the validators are processing transactions correctly and ensures that the network will always achieve consensus despite dishonest node operators.

In addition, all databases operated by Hedera Validators are ACID (Atomicity, Consistency, Isolation, Durability) compliant because each node stores transactions locally following the consensus order, and all nodes share the same properties.

Finally, the Hedera Network is resistant to DDoS attacks because the network is sufficiently distributed to make DDoS attacks on the entire network prohibitively costly.

3.3.4. Production-Ready Environment Costs for UDPN Nodes

During this PoC, the UDPN builders estimated the requirements and costs of running most UDPN nodes (Business Node, Validator Node, and Transaction Node) in a cloud instance. For this example, we used an AWS estimation tool covering three regions where our target users are located.

The recommended specifications to run a UDPN node are listed below:

- Instance Type: t4g.2xlarge (8 vCPU, 32 GiB RAM)
- EBS Storage: 500 GB (gp3)

Most of the cost is taken up by computing, which can vary significantly depending on the target deployment region. For example:

Region	Estimated Annual Cost/UDPN Node
APAC – Singapore	3,500 USD
US East – N. Virginia	2,800 USD
Europe – Frankfurt	3,200 USD

Table 7: Estimated Infrastructure Costs by Region

Note: *These costs are estimates based on on-demand pricing. Using AWS Savings Plans can significantly reduce costs (up to 60-70% with a 3-year commitment). In addition, considering other cloud service providers and on-prem hosting solutions could generate significant infrastructure cost savings.*

Copyright © 2024 UDPN. All rights reserved.

On top of the base cost of provisioned compute resources, a production setup would require considering the following:

- **Failover Mechanisms:**

Depending on the Recovery Time Objective (RTO) goal, failover mechanisms may involve running a standby replica of all services at all times, which effectively doubles the compute resources needed.

- **Snapshots/Backups:**

When considering an incremental snapshot mechanism and using a regionally resilient service like Amazon S3, the cost varies based on actual usage (which is determined by the incremental change to the data stored), region, and storage class used. The price may range from 0.005 USD to 0.025 USD per GB stored, considering only storage classes suitable for instant retrieval.

- **Observability Platform:**

The nature of the observability platform depends on the solution within the client's environment. For example, basic observability, which involves collecting logs, metrics, traces with simple dashboards, and alerting available through AWS CloudWatch, may cost less than 50 USD per month. Custom solutions may include additional hosting/license fees.

- **Managed Services:**

Managed services can be used in a production environment to reduce administrative overhead or meet specific requirements, such as global resiliency. This can be especially beneficial for services like databases, queues, or k8s clusters.

3.4. Money Transmission & Privacy Considerations

3.4.1. UDPN's Responsibilities as a Messaging Infrastructure

The UDPN Alliance members do not exercise any control over the digital currencies transmitted via the network because the UDPN underlying smart contracts and blockchain constitute a messaging infrastructure, and they do not have access to the private keys used to sign digital currency transactions.

Money transmitters can leverage the UDPN infrastructure to streamline their operations, such as transferring digital currencies between two accounts or ensuring compliance with the Travel Rule by leveraging a single set of APIs and applications deployed on the UDPN underlying blockchain. However, money transmitters always remain in control of their digital currencies and must comply with all applicable laws and regulations in their jurisdictions. The APIs provided to interact with the UDPN messaging infrastructure simplify the money transmitters' interactions with digital currencies but do not prevent them from complying with the law.

Like SWIFT, if the UDPN is used to transmit money for fraudulent or unlawful purposes,

Copyright © 2024 UDPN. All rights reserved.

the UDPN Alliance Members will voluntarily support investigations. Indeed, the network was designed to help regulators oversee transactions via the Transaction Audit & Reporting Node, where transaction data is available in real-time.

3.4.2. Data Privacy

Personal information is neither stored nor transferred on-chain to safeguard data privacy. Instead, all personal information is stored off-chain, and only the Business Node operators retain the end users' personal information during their internal KYC processes. When a transaction message is validated on the UDPN network, Validator Nodes and Transaction Audit and Reporting Nodes access limited information, such as the DID identifiers of the originator and beneficiary, the currencies used, the currency amounts, and the currency systems involved in each swap or transaction. This approach ensures that data privacy is effectively managed by the Business Node operators, further enhancing data privacy and optimising transaction speed.

Copyright © 2024 UDPN. All rights reserved.

4. Conclusion

This UDPN PoC showcased one of the first digital currency transfers and swaps on a high-performance network. The UDPN efficiently connects digital currency systems for seamless cross-border and cross-network payments. During this PoC, two additional Transaction Nodes were integrated into the UDPN: one supporting stablecoins issued with the Stablecoin Studio, connecting directly to the Hedera network via Hedera SDK and the other supporting EMTECH CBDCs via their Digital Cash platform.

The transaction confirmations were noticeably faster than on other networks, highlighting this PoC's potential for commercial applications where transaction execution and settlement must be achieved in real-time. The UDPN empowers businesses and financial institutions to utilise regulated digital currencies effectively in payment applications. The UDPN ensures data privacy and encourages broader adoption by maintaining a decentralised and secure architecture.

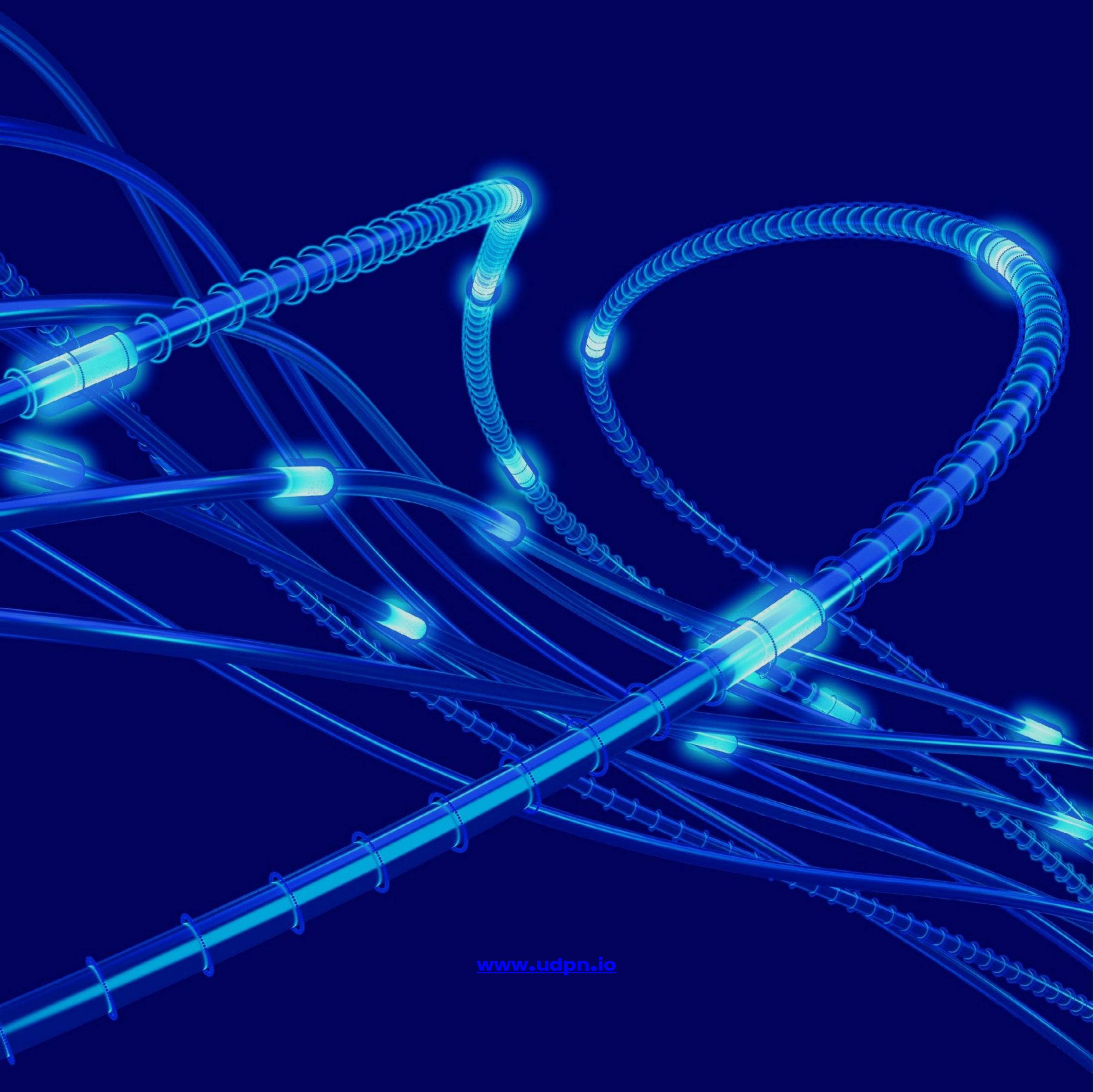
The PoC outcomes demonstrate UDPN's potential to simplify integration processes, reduce costs, and increase transaction speed in the digital payments landscape. As the network progresses, regulatory considerations and compliance will remain critical for its success. Overall, the UDPN promises to reshape the future of digital payments and financial transactions.

Copyright © 2024 UDPN. All rights reserved.

Acknowledgements

We sincerely thank the HBAR Foundation for funding this PoC through their Grant Programme. The development of this Proof-of-Concept and the writing of this report would not have been possible without their help. We also would like to take the opportunity to thank Sabrina Tachdjian (HBAR Foundation) and Pathorn Tengkiattrakul (Swirlds Labs) for taking the time to answer our questions and expand our understanding of the Hedera Ecosystem. We hope this report will be helpful to the community and provide further insights into the value of the UDPN and Hedera Networks. We eagerly anticipate future opportunities for cooperation with both institutions as we continue to advance our journey toward the commercialisation of the network.

Copyright © 2024 UDPN. All rights reserved.



www.udpn.io