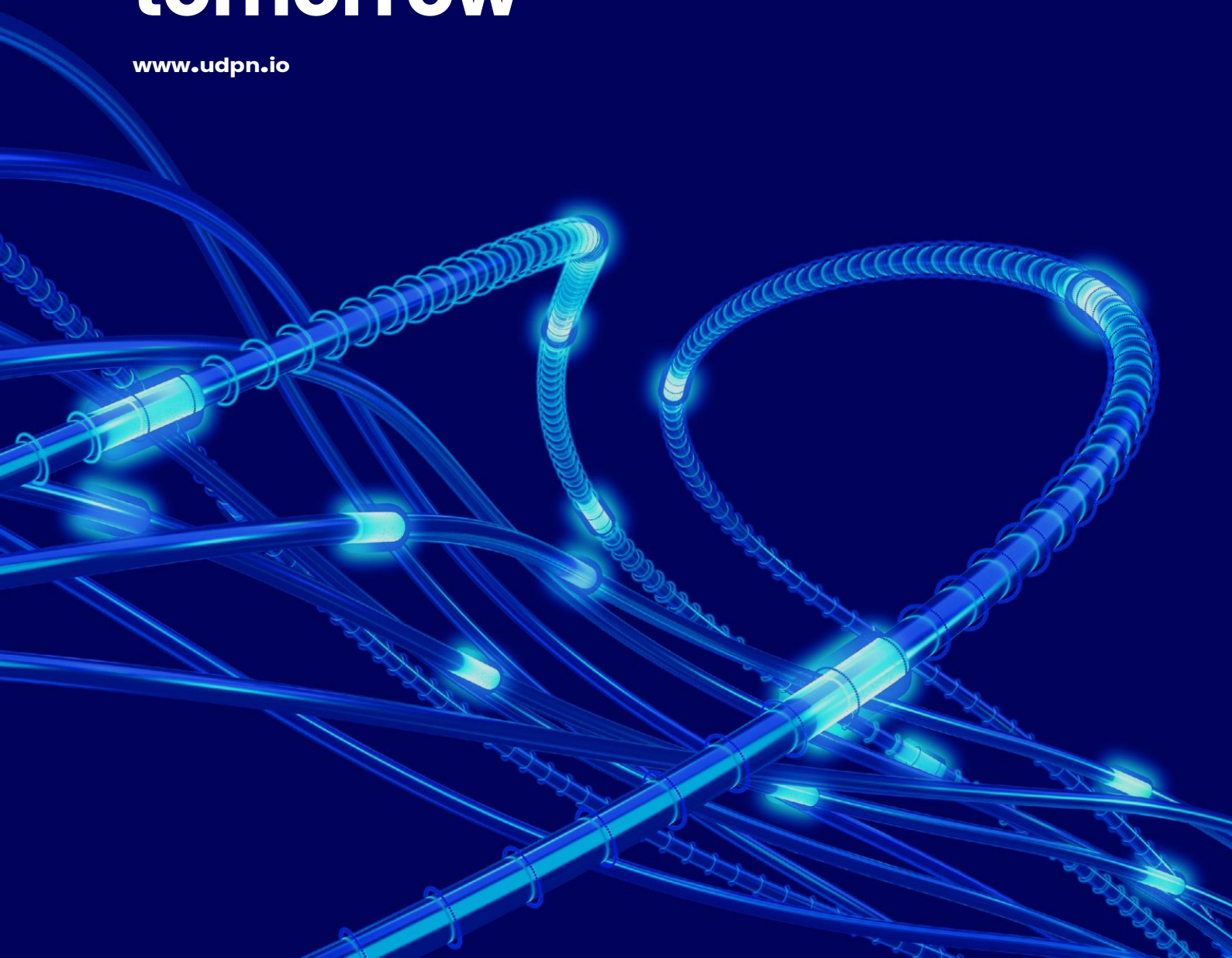




Universal Digital Payments Network

Interoperable payment infrastructure for the digital currencies of tomorrow

www.udpn.io



EXECUTIVE SUMMARY

As an ever-increasing number of CBDCs and regulated stablecoins come online, the need for interoperability grows. The UDPN meets this need, offering lower payment costs and rapid, seamless distribution.

The last few years have seen a fundamental shift across the financial sector, driven by the need to promote financial inclusion, increase competition and modernise decades-old payments infrastructures. The proliferation of FinTech and digital commerce is giving individuals and companies ever-increasing levels of control over their financial accounts whilst prompting companies to process digital payments in a standardised and cost-efficient manner. In response, central banks around the globe are re-thinking how to structure their respective currency systems, leading to fundamental changes in how commercial banks intermediate payments.

The global payments ecosystem is seeing a rise in the development of digital currencies, including an increase in both occurrence and use of regulated, fiat-backed stablecoins. There is also a rapidly growing body of research & development being undertaken by central banks into Central Bank Digital Currencies (CBDCs). These digital currencies offer many benefits: improved ease and speed of transactions, improved transparency and liquidity, enhanced resilience and security, reduced costs, and increased access to money (including to underbanked and unbanked populations).

Despite the surge in interest, there is no agreed messaging standard across digital currencies (such as ISO20022 for traditional payments), which threatens to hinder the adoption of stablecoins and CBDCs. Incumbent legacy infrastructure aside, the challenge of interoperability between different digital currency protocols is currently the most significant hurdle facing the development of digital currencies globally. Scalable and universal interoperability will be key to enabling the efficient movement of digital currencies between the legacy payments infrastructure and the rapidly evolving digital currency systems. Interoperability will be necessary between different CBDCs, as well as between CBDCs and stablecoins.

The UDPN addresses these issues by providing a global payment messaging network to support stablecoins and CBDCs across decentralised and centralised currency systems. The UDPN will provide a shared, decentralised network and associated standards; the messaging backbone for efficient and seamless cross-border digital currency payments across protocols and systems.

KEY FEATURES AND BENEFITS OF THE UDPN INCLUDE:

1. A common standard for messaging across different digital currency systems, facilitating interoperability functions between CBDC and stablecoin ecosystems.
2. Enables all types of commercial enterprises globally to transact and settle in different currencies, allowing them to easily integrate with multiple digital currency payment systems. Connection to the UDPN is achieved via locally installed Business Nodes that provide access to the network and thus connect users to the associated CBDC and stablecoin currency systems.
3. Provides core digital infrastructure services to any IT system that can offer applications and services involving digital currency payments, in a comparatively low-cost and convenient manner. The UDPN does not serve individual end users directly.
4. The network will support only CBDCs and regulated fiat-backed stablecoin currency systems as payment methods. No unregulated public-chain cryptocurrencies, such as Bitcoin, will be accepted. The addition of any new currency is subject to a vote by the UDPN Alliance members as part of the network's decentralised governance approach. A core objective of the UDPN is to work within a regulated landscape designed for payment services; crypto assets, or non-regulated stablecoins cannot be adopted universally (even at a regional level) for this purpose and are therefore not supported by the network.
5. Accelerated access for commercial banks to actively participate in the decentralised economy. Banks will be able to provide capital pools and engage with local central banks to offer liquidity for cross-border foreign exchange transactions.
6. Management by an alliance of financial institutions and technology companies from different countries and industry verticals, each having shared equal ownership of the network to promote an inclusive and robust governance structure.
7. The UDPN does not provide custodial services, nor does it hold or move any digital currencies.
8. A permissioned network with four primary nodes: the Validator Nodes and Transaction Audit & Reporting (TAR) Nodes are on-chain, whereas the Business and Transaction Nodes are off-chain. The Validator Nodes contain the Hyperledger BESU peer, validator and governance systems. The TAR Nodes contain the BESU Archive Node, which can provide relevant transaction data to support regulatory requirements from governments or central banks. Business Nodes connect IT systems to the UDPN, whilst Transaction Nodes connect different stablecoin, CBDC systems, and capital pools.
9. Each node has a distinct set of attributes and is run by different stakeholders, including commercial enterprises, regulated financial institutions, regulators and UDPN Alliance members.
10. The beta release of the UDPN is scheduled to go live with two to five stablecoins in Q4 2022, with pilot commercialisation by mid-2023. In the medium to long term, the UDPN should support the majority of the world's CBDCs and regulated, fiat-backed stablecoins.
11. Transaction messaging between various account systems. The UDPN has been designed for CBDCs and stablecoins, however, technically it could be extended to support messaging with traditional messaging systems.

At launch, 8 UDPN Alliance members will form the initial core group of founders, expanding to 16 and then 24 members over the succeeding two years. This international Alliance will lead development of the roadmap, standards, governance, and commercialisation strategy for the UDPN, through a vote-based decision-making process.

The UDPN is designed for both the present and the future. With CBDCs and stablecoins anticipated to become integral to the cross-border payments ecosystem, the UDPN is ideally placed to become a primary channel in the digital currency distribution model of central banks. The same is true for those looking to transfer or swap digital currencies, whether they be enterprises, financial services firms, businesses or individuals. Supported by the UDPN, the evolving payments ecosystem can move towards a vastly improved and more resilient future, which is in sync with the development of emerging technologies.

ACKNOWLEDGEMENTS

CHAVANETTE ADVISORS

Alexander Feenie

GFT

David Creer

FINSTEP ASIA

Syed Musheer Ahmed

RED DATE TECHNOLOGY

Yifan He

CONTENT

1. INTRODUCTION	7
1.1. BACKGROUND	7
1.2. OBJECTIVES OF THE UDPN	10
2. HIGH LEVEL ARCHITECTURE & OPERATIONAL MODEL	12
2.1. HIGH LEVEL UDPN ARCHITECTURE	12
2.2. PERMISSIONED DECENTRALISED NETWORK	12
2.3. STAKEHOLDERS AND NODE TYPES	13
2.3.1. UDPN Decentralised Identity (DID)	13
2.3.2. UDPN Nodes	14
2.3.3. Smart Contracts	18
3. TRANSACTION FLOWS	20
3.1. CREATION OF UDPN DIDs	20
3.2. LINKING/DE-LINKING DIGITAL CURRENCY ACCOUNTS TO UDPN DIDs	21
3.3. DIGITAL CURRENCY TRANSFERS & SWAPS (FX)	23
3.4. REFUND PROCESS IN THE CASE OF A FAILED TRANSFER	24
4. WHOLESALE DIGITAL CURRENCY SETTLEMENT	26
5. SECURITY AND PRIVACY	27
5.1. IT SECURITY	27
5.2. NETWORK SECURITY	29
5.3. PRIVACY	31
5.4. KNOW YOUR CUSTOMER (KYC) RULES	32
6. REGULATORY COMPLIANCE	33
7. UDPN ALLIANCE & GOVERNANCE	34
7.1. ORGANISATION & FOUNDING MEMBERS	34
7.2. DECENTRALISED GOVERNANCE AND VOTING	34
7.3. REVENUE MODEL	35
8. SOCIAL IMPACT	36
9. ROADMAP	37
10. CONCLUSION	38

1. INTRODUCTION

1.1. BACKGROUND

In a world driven by technology, we are witnessing a major transition in the way that central banks, financial institutions, and end users conduct financial transactions. The advent of SWIFT in the early 1970s enabled and facilitated a significant rise in cross-border, bank-to-bank financial transactions, which now run into trillions of dollars every day. Although revolutionary at the time, this cross-border payment set-up is not compatible with the rapid changes coming from the evolution of the finance industry. Innovations in FinTech, digital currencies and decentralised finance demand a new standard for transactions and payments, which is faster, safer and programmable. The rapid transformation of the payments industry presents businesses with new opportunities to assist their customers in their payment processes using a broad range of new innovative technologies (such as Distributed Ledger Technology), providing payment efficiencies at a low cost. Regulated financial services institutions and FinTechs have the opportunity to play a vital role in the future of digital currencies, from facilitating the distribution of CBDCs to reducing settlement risks.

Today, cross-border transactions represent 15-20% of total e-commerce activity and this share is expected to grow substantially in the coming years¹. Annual remittances exceeded US\$700 billion in recent years² and despite a short term drop in international travel due to the Covid-19 pandemic, international migration and travel have grown by 53% in the last decade, placing further demand on cross-border payment infrastructures³.

Cross-border payments today are subject to slow processing and high costs due to the fragmented nature of the correspondent banking model. Payments are routed through chains of correspondent banks, using legacy systems that lack real-time capabilities when dealing with transactions across segregated monetary zones, creating significant delays, inefficiencies and additional costs⁴.

**CROSS-BORDER
PAYMENTS TODAY ARE
SUBJECT TO SLOW
PROCESSING AND HIGH
COSTS DUE TO THE
FRAGMENTED NATURE
OF THE CORRESPONDENT
BANKING MODEL.**

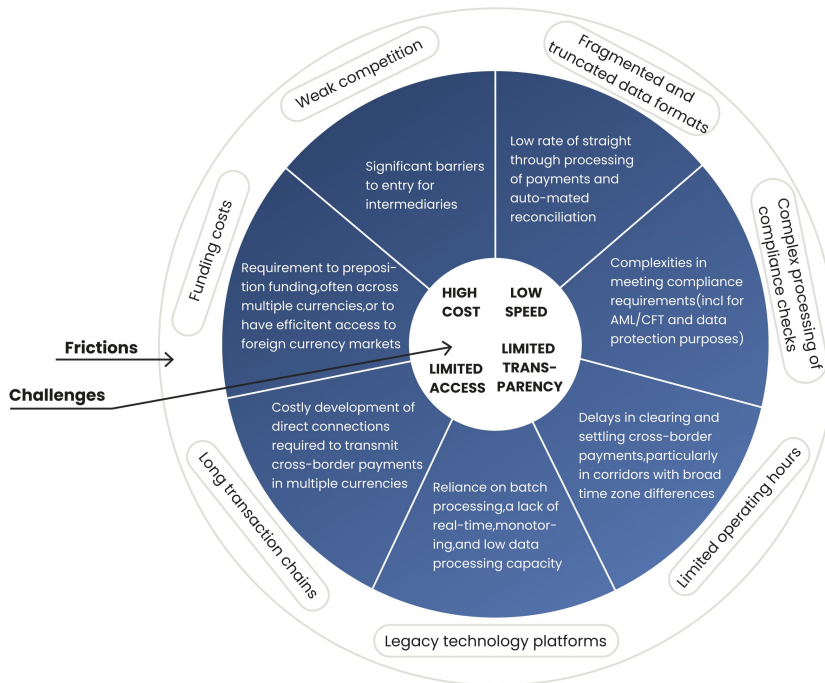
¹McKinsey (2018) <https://www.mckinsey.com/industries/financial-services/our-insights/a-vision-for-the-future-of-crossborder-payment>

²<https://www.knomad.org/data/remittances>

³UN World Tourism Organization (2020). <https://www.unwto.org/world-tourism-barometer-n18-january-2020>

⁴<https://www.rba.gov.au/speeches/2019/sp-gov-2019-12-10.html> - Graph 6

Figure 1. Challenges and frictions in cross-border payments



Source: CPMI based on FSB (2020b)

Fees average 7% for cross border remittances, with inter-bank fees reaching over 11% in some cases⁵. Additionally, both businesses and individuals have only limited transparency of the full fee and transaction timelines, making cash-flow management cumbersome and increasing unpredictability related to sending and receiving payments.

The rise of the smartphone has brought about an exponential increase in mobile payments globally. FinTech firms are disrupting the traditional market, utilising digital technologies to lower costs and increase the speed of transactions. The increasing popularity of wearable technologies and contactless payments (further bolstered by an increased focus on hygiene during the Covid-19 pandemic) is expected to increase the number of people favouring digital payment methods over physical cash. The move from cash to cashless is expected to become omnipresent for consumers everywhere in a few years. Four in five (83%) Europeans say (to varying degrees) that they use cash less often since they have started to use contactless payments, illustrating how technology is influencing behaviour⁶. In the UK, usage of cash dropped from 63% in 2006 to 28% in 2018⁷. Many places globally, including Sweden and a significant portion of urban China, have already turned almost entirely cashless.

In parallel to this growth in digital payments, the last five years have also seen a significant rise in the development and use of Distributed Ledger Technologies (DLT) for conducting payments. Financial institutions, including central banks,

⁵<https://www.worldbank.org/en/news/press-release/2019/04/08/record-high-remittances-sent-globally-in-2018>

⁶<https://think.ing.com/articles/not-even-a-global-pandemic-can-shift-preferences-for-cash-as-an-option>

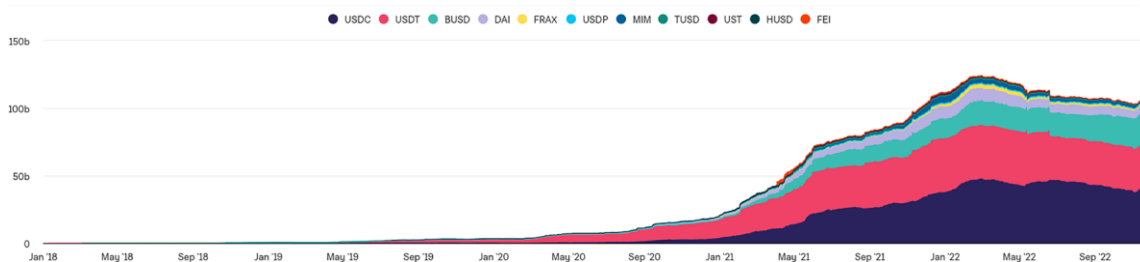
⁷<https://www.bankofengland.co.uk/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design-discussion-paper>

have embraced the value of using digital currencies for cross-border payments, thereby enabling a more efficient approach for transacting outside of the more traditional payment systems. The development of stablecoins and Central Bank Digital Currencies (CBDCs) offers many benefits. These include enhanced liquidity, significant cost savings, superior transparency, higher resilience, improved speed, ease of transactions and improving the access to money (including to the underbanked and the unbanked).

These digital currencies will soon be embedded in all aspects of the financial system, from e-commerce and retail payments to wholesale payments and securities transactions. In the smart cities of the future, payments will be everywhere, anytime, digital and in real-time. The future of money will be completely transformed. To meet the demand from businesses and consumers, banks need to evolve beyond the existing infrastructures, such as SWIFT, and innovate and adopt connectivity to new digital currencies. Regardless of the distribution model central banks choose to deploy, CBDCs will change banks' clients' relationship with money. Banks, therefore, need to innovate and adapt, implementing new business models to meet the changing needs of their customers.

As with the evolution of most new technologies, we have seen a host of different solutions being used to build these new payment rails. Additionally, there is growing use of stablecoins as a means of bridging the gap between the world of digital currency with that of fiat money. The overall digital currency space is growing at a rapid pace, with over US\$60 Billion in stablecoins and over US\$300 million in CBDC transaction volumes already recorded⁸.

Figure 2. Total stablecoin supply YTD (29/06/2022)

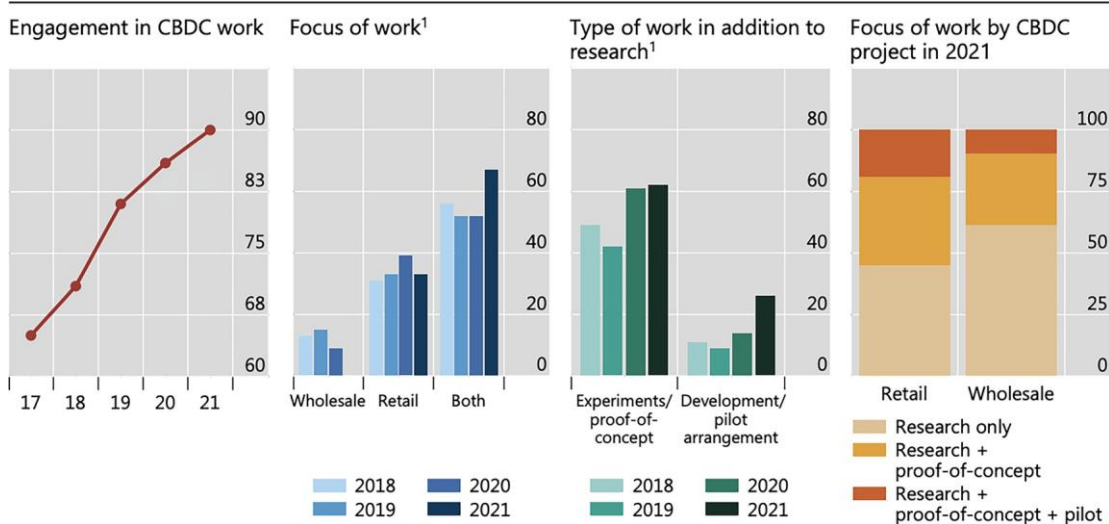


Source: Coin Metrics. The Block

Globally, most central banks are now actively engaging in the CBDC space with varying degrees of progress. As per a BIS survey⁹ of 65 central banks, 86% said they had completed some work on the topic, while 60% are conducting experiments or proof-of-concept studies (up from 42% in 2019), and 14% are moving forward with development and pilot arrangements.

⁸<https://www.pwc.com/gx/en/industries/financial-services/assets/pwc-cbdc-global-index-1st-edition-april-2021.pdf>
⁹Ready, steady, go? – Results of the third BIS survey on central bank digital currency

Figure 3. CBDC exploration and development
Share of central bank respondents - Central bank involvement in CBDC work rises further



¹ Share of respondents conducting work on CBDC's
 Source: 2021 BIS Central Bank Survey on CBDC's and digital tokens.

1.2. OBJECTIVES OF THE UDPN

Scalable and universal interoperability will be vital to efficiently move digital currencies between the legacy payments infrastructure and the rapidly evolving digital currency infrastructure. The Universal Digital Payments Network (UDPN) addresses this need 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 fragmented ecosystems, leveraging advances in blockchain infrastructure to connect both stablecoins and CBDCs. The goal of the UDPN is to create a decentralised network and associated standards to improve efficiency in cross-border payments processing. The UDPN will enable enterprises from different countries to transact and settle in different regulated digital currencies by merely accessing their locally installed Business Nodes. Furthermore, the UDPN provides a way for commercial banks to participate in the decentralised economy.

Just as the SWIFT network (linking more than 11,000 financial institutions across 200 countries and territories) created the original common 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 DLT for multi-party coordination and 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 on the network for clearing and settlement purposes. Instead, the UDPN will

operate as a network that connects different digital currencies, working with multiple stakeholders and becoming the messaging backbone between various CBDC and stablecoin systems. The objective of the UDPN is to facilitate central bank and fiat-backed digital currency systems globally to connect to a wide distribution network of regulated institutions and IT systems.

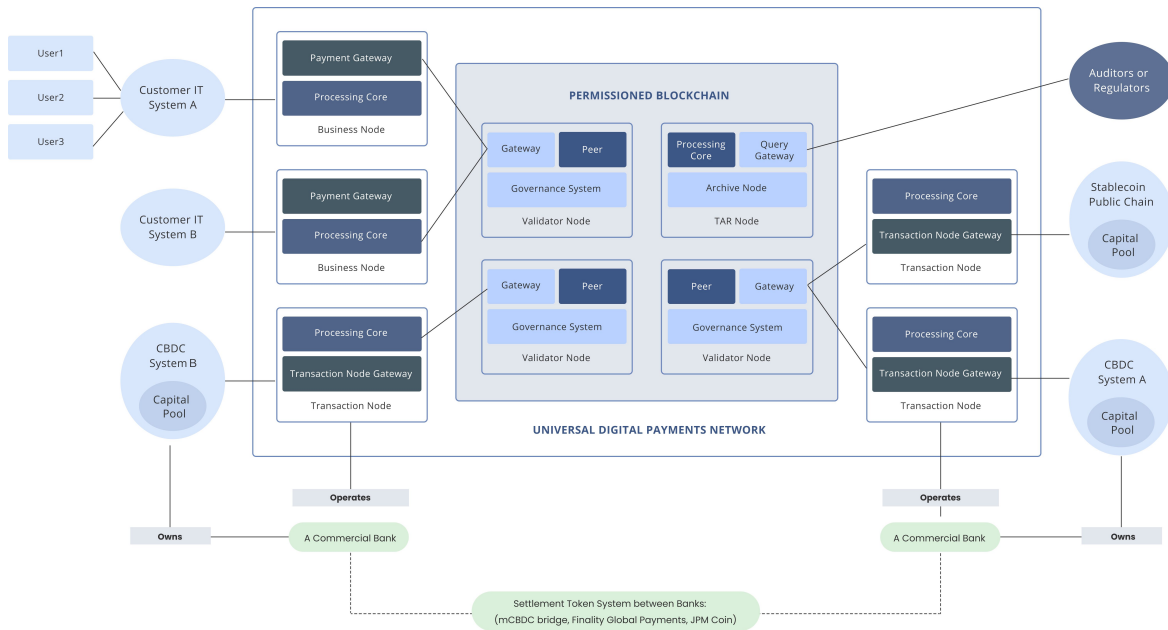
The UDPN will only support CBDCs and stablecoins as payment methods and will not support transactions involving any unregulated, public-chain cryptocurrency such as Bitcoin. All transactions will still occur within each CBDC or stablecoin system. For this reason, the UDPN does not provide any custodial services or hold any digital currencies itself. Instead, the UDPN provides critical universal messaging and interoperability functions to all CBDC and stablecoin ecosystems.

Critical to achieving a common international infrastructure for cross-border payments is a governance model that allows stakeholders from all countries to participate in the network's use, development, operation, and maintenance in a trusted and equitable way. It is the goal of the UDPN to develop an inclusive framework to address the issues of governance, ownership, and participation in a network leveraging DLT. The UDPN will be managed by an alliance of financial institutions and technology companies from different countries and industry verticals, each with shared equal ownership of the network to promote an inclusive and robust governance structure.

2. HIGH LEVEL ARCHITECTURE & OPERATIONAL MODEL

2.1. HIGH LEVEL UDPN ARCHITECTURE

Figure 4



2.2. PERMISSIONED DECENTRALISED NETWORK

The primary objective of the UDPN is to provide a messaging layer for global cross-border payments of CBDCs and stablecoins. With most businesses being off-chain, the UDPN structure has been built to link business IT systems with centralised and decentralised currency systems, using Hyperledger BESU as the permissioned network framework.

The foundational architecture of the network is a permissioned, decentralised network of on-chain Validator Nodes, engaging with off-chain Business and Transaction Nodes. Off-chain Transaction Nodes operated by commercial banks will securely connect central banks and stablecoin systems issuing digital currencies to the UDPN, while Business Nodes will allow any business system to connect to the UDPN. In addition, the on-chain Transaction Audit and Reporting (TAR) Nodes facilitate the work of regulators and auditors in monitoring the transactions of their respective digital currencies.

The UDPN is primarily a messaging platform and does not compete with currencies in circulation or issue tokens. It will have decentralised IDs (DIDs) linked with the

digital wallets or accounts in the corresponding public chains or CBDC systems. All transactions are performed within each currency system, and shared data is kept to a strict minimum (maintaining the privacy of users). The UDPN network thus has the advantage of being light on data and as such, aims to support at least two thousand transactions per second at launch.

The UDPN will not provide any custody services, nor will it hold or move any digital currency. It will operate on the assumption that digital currency holders' transaction and settlement information is true, accurate, complete and genuine, and therefore not bear any obligation nor liability in this regard.

The UDPN architecture is robust and built with security in mind. The data-driven framework enhances the performance of transactions and ensures that the infrastructure adheres to the highest standards of operational resilience. The UDPN will deploy an integrated and comprehensive approach to mitigate any challenges to the network and ensure the system is reliable, resilient and efficient at all times. The network will be subject to regular and stringent contingency tests, to ensure continuity of operation.

In addition to business continuity planning, the multi-layered frameworks counter any system disruption, ensuring that backups are always in place. The system design is modular and scalable to serve an ever-increasing number of participants and transactions. UDPN stakeholders will be engaged in the ongoing risk management of the network to ensure the resilience of their systems and compatibility with all UDPN upgrades and risk management measures

2.3. STAKEHOLDERS AND NODE TYPES

The UDPN does not serve individual consumers directly but rather provides digital infrastructure core services to businesses and financial institutions, which can build applications and services involving digital currency payments. Any business could facilitate transactions in CBDCs and stablecoins on the UDPN by installing an open-sourced UDPN Business Node.

Businesses include any commercial enterprise, from commercial banks and IT vendors to E-commerce players and FinTechs facilitating payments. Capital pools managed by licensed money service providers, such as commercial banks, will facilitate the exchange of stablecoins and CBDCs. The UDPN network itself will not directly operate any capital pools.

2.3.1. UDPN Decentralised Identity (DID)

The UDPN enables any entity or individual to build applications and services involving digital currency payments in a low-cost and convenient manner. These IT systems can establish Business Nodes after receiving permission from Validator Nodes to become an access point on the UDPN. To onboard end users, the Business Nodes will need to create unique UDPN decentralised IDs (DID) linked with existing accounts

can establish Business Nodes after receiving permission from Validator Nodes to become an access point on the UDPN. To onboard end users, the Business Nodes will need to create unique UDPN decentralised IDs (DID) linked with existing accounts and wallets on CBDC and stablecoin systems. The businesses can decide whether to create one DID for each end user or use their own DIDs for multiple accounts or users.

The decentralised UDPN network will create a digital identity contract that will have the details of the DID and provide DID services to UDPN network members. A DID resolver will provide a DID resolution service that connects to DIF's (Decentralized Identity Foundation's) Universal Resolver.

User credentials are securely stored in the identity hub within a Business Node. An issuer registration service will be enabled to publish the UDPN network member list and the Transaction Node owner list, along with their issuable credentials. The other functions of this service include input, delete and query of the issuer information. To maintain data privacy, the DID will not include the personal information of the end user. Only IT systems have the personal information of the end users that they onboard, as part of their relevant KYC process.

Lastly, a credential issuing service will be enabled to define unified, standard credential issuing service APIs. Issuers (UDPN Alliance members and Transaction Node owners) will implement and manage their own credential issuing services using UDPN's standardised credential management APIs. The main APIs include those used to apply for credentials, obtain application results, and query a credential revocation list.

2.3.2. UDPN Nodes

The UDPN permissioned network has four main nodes: The Validator Nodes and TAR Nodes are on-chain, whereas the Business and Transaction Nodes of the UDPN are off-chain. The Validator Nodes contain the Hyperledger BESU peer, validator and governance systems, with the TAR Nodes containing the BESU Archive Node. In every node, digital identity services integrate the UDPN DID client SDK to achieve DID management, DID resolution, issuer registration services, credential management, and data encryption storage management.

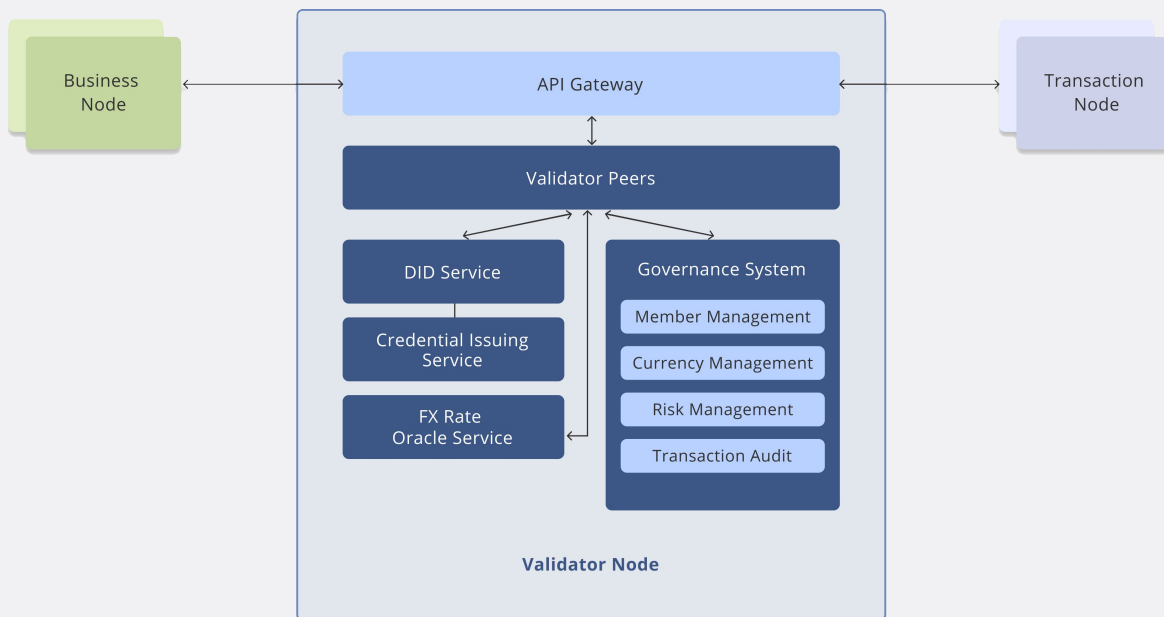
1. Validator Nodes: The Validator Nodes are at the heart of the UDPN. A cluster of Validator Nodes connected with all other stakeholders via a secure and encrypted connection will validate any transaction on the UDPN. The Validator Nodes and TAR Nodes are the only nodes that store a complete set of transaction data on the UDPN. The Validator Nodes' code will be open-source, owned and operated exclusively by the UDPN Alliance members to ensure proper transparency.

Validator Nodes only validate the format of the message received from a certified Business Node. Upon receipt of a message, the Node validates the veracity of the signature and message origin. It does not, however, validate the content of the message. The content is only validated by the currency systems, depending on the

nature of the transaction.

Each Validator Node's operations are conducted with full autonomy. Network operations and governance are driven using a majority-based voting consensus mechanism. All the Validator Node owners will have the right to vote on such topics as network access permissions, the performance of software updates, the approval of new smart contract deployment and adjustments to fee structures.

Figure 5



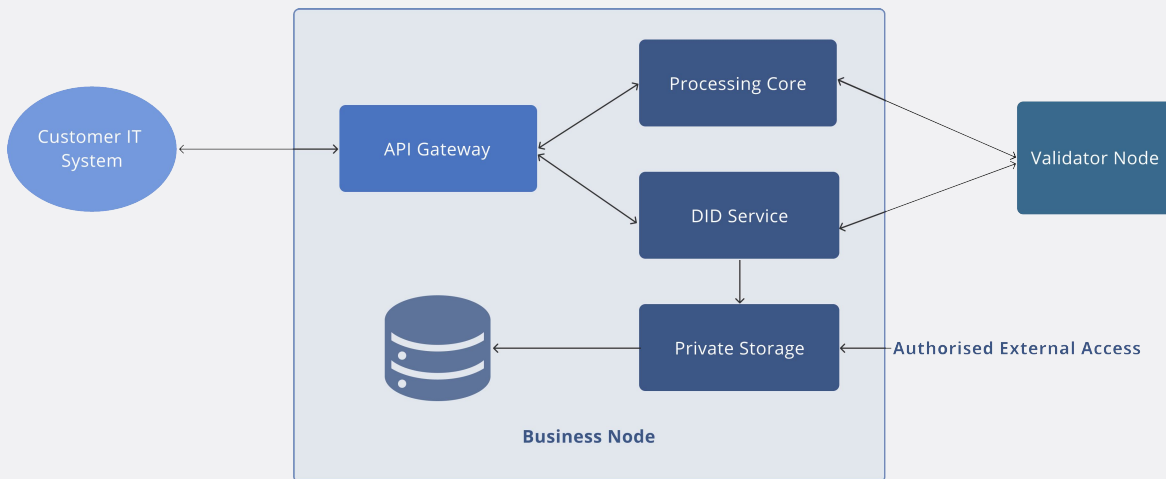
All Validator Nodes contain a governance system that ensures adherence to the rules of the UDPN. As there will be multiple Validator Nodes in the network, with more being added as the Alliance grows, not all Validator Nodes are required to participate in the same transaction. Each transaction submitted from the Business Nodes will be randomly assigned to certain Validator Nodes to validate. All transactions are validated and written to the peer of the Validator Node, which reads, endorses, and writes transactions to the blockchain ledger. The Validator Nodes are connected to the Business and Transaction Nodes through APIs.

Validator Nodes should be installed in the members' own cloud account or on-premises infrastructure. As part of the Validator Node installation, each member will also install the UDPN governance software, which is used for voting. The governance platform is a separate system connected to the network, with on-chain controls, as an integral part of the Validator Node.

2. Business Nodes: The UDPN does not serve individual end users directly. The end users interact with the UDPN through Business Nodes, owned and set up by businesses who wish to integrate UDPN services into their business systems. All Business Node owners must undergo a strict KYC check before connecting to the UDPN. Like

the Validator Nodes, the code for the Business Nodes is open source, and IT system administrators can download the code and install it on their systems locally.

Figure 6



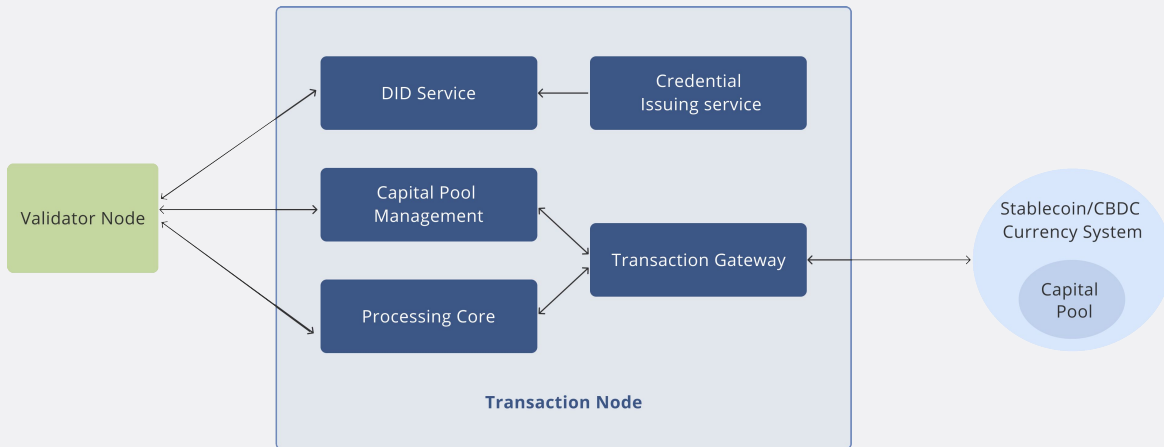
To onboard a Business Node, the businesses owning the IT systems need to submit an application. Once approved by the Validator Node's governance system, the Business Node is added to the UDPN, and a certificate and a DID created for the Business Node.

Each Business Node contains a gateway and private storage and only stores its own UDPN transaction data. A digital identity service integrates the UDPN DID client SDK. To conduct payment services, the Business Node will interact with the UDPN network to initiate a currency transfer or swap request and support querying the state of its transactions.

The IT system uses gateway APIs to access the Business Node. This API gateway provides the unified encapsulated digital identity management and payment transaction processing services of the Business Nodes. Everything in the private storage is encrypted by a Business Node private key. The private storage contains the credentials issued by UDPN issuers or currency systems along with storing off-chain private data, such as that related to KYC. To access credentials, other DIDs need to be granted permission by the Business Node owner.

3. Transaction Nodes: These nodes are custom made for each currency, with the possibility of there being multiple Transaction Nodes per currency to handle a high volume of transactions. The most important aspect of the Transaction Node is connectivity with the currency system, especially where that currency system is a CBDC system requiring KYC. Transaction Nodes can only be operated by regulated and licensed money service providers, primarily commercial banks.

Figure 7



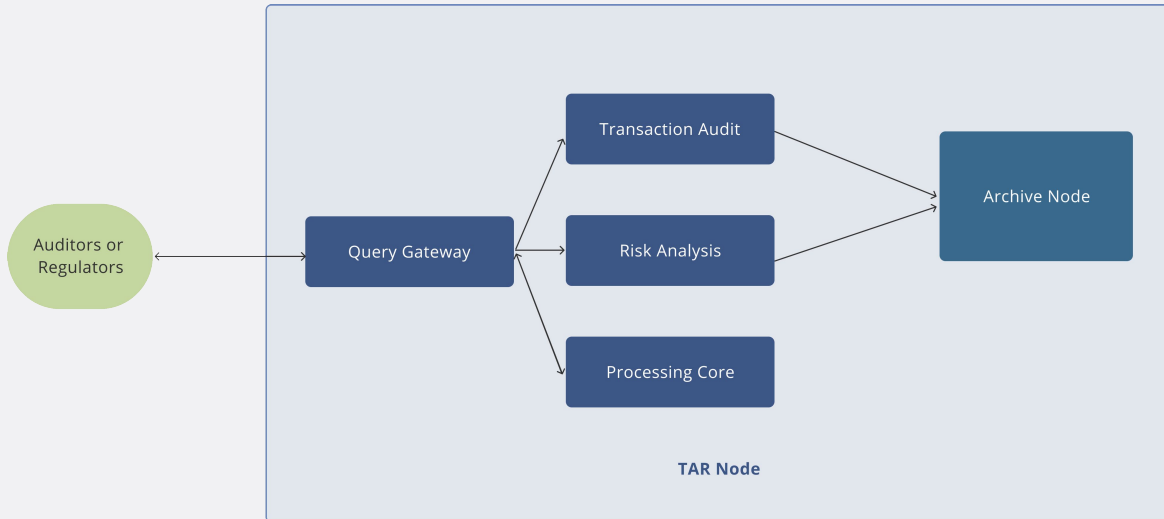
Each Transaction Node will contain a capital pool management module for currency swap operations, thereby providing deep liquidity for all currency pairs. They will connect to the digital currency systems through the transaction gateway for transfer, transaction and query results. Transaction Nodes could be integrated with traditional settlement systems (such as RTGS, CHAPS or Target2) so that they can manage liquidity in their capital pools.

Customised development is required for each currency on the network. This is based on the respective currency system requirements for verifications and transactions. Once a transaction that has been initialised on the UDPN is validated, it will be passed to the corresponding digital currency systems. For account-linking operations, the relevant Transaction Node will issue a signed certificate, and the related Business Node will store these credentials once the currency system successfully verifies the ownership of the account.

The requests and responses regarding certificates will be handled off-chain and enhanced by multiple layers of secure processing. It is worth noting that both the Business Nodes and Transaction Nodes store only the data they have processed and not the rest of the network data. This approach enhances data privacy and increases transaction speed.

4. Transaction Audit and Reporting (TAR) Nodes:

Figure 8



The TAR Nodes are installed on-demand to facilitate the work of regulators and auditors in monitoring transactions on the network. Regulators and auditors are allowed to query data from the Archive Nodes. They can also install applications on top of the TAR Node to further ease transaction monitoring and Risk Analysis. The TAR Nodes can only query data and cannot input any data onto the network.

The TAR Nodes hold the same data as the Validator Nodes. This data does not include any end user personal information other than DIDs, currency types, transaction amounts and some scrambled currency account numbers. Authorities must also seek permission from their own currency's Transaction Node owners to access any additional data.

2.3.3. Smart Contracts

Each operation on the UDPN is defined by a set of smart contracts enabling the automation of settlement and compliance processes. The UDPN supports Solidity smart contracts deployed to a Hyperledger BESU permissioned network. Any new business operations can be added through the deployment of new smart contracts. These smart contracts can only be deployed and updated on the UDPN upon receipt of approval from the operators of the Validator Nodes.

The smart contracts are deployed across a host of activities and transactions, currently including:

- DID contract
- Issuer registration contract
- Account or wallet linking/delinking contract
- Currency registration contract
- Payment processing contract
- FX Exchange match-making contract
- Authority Management contract (for access control)
- UDPN governance contract
- Revenue distribution contract

3. TRANSACTION FLOWS

The UDPN facilitates the flow of payment transactions through a combination of on-chain and off-chain processes, with only the Validator and TAR Nodes being on the permitted DLT network. As previously mentioned, the end-user engages with the UDPN via the IT systems of the UDPN direct customers.

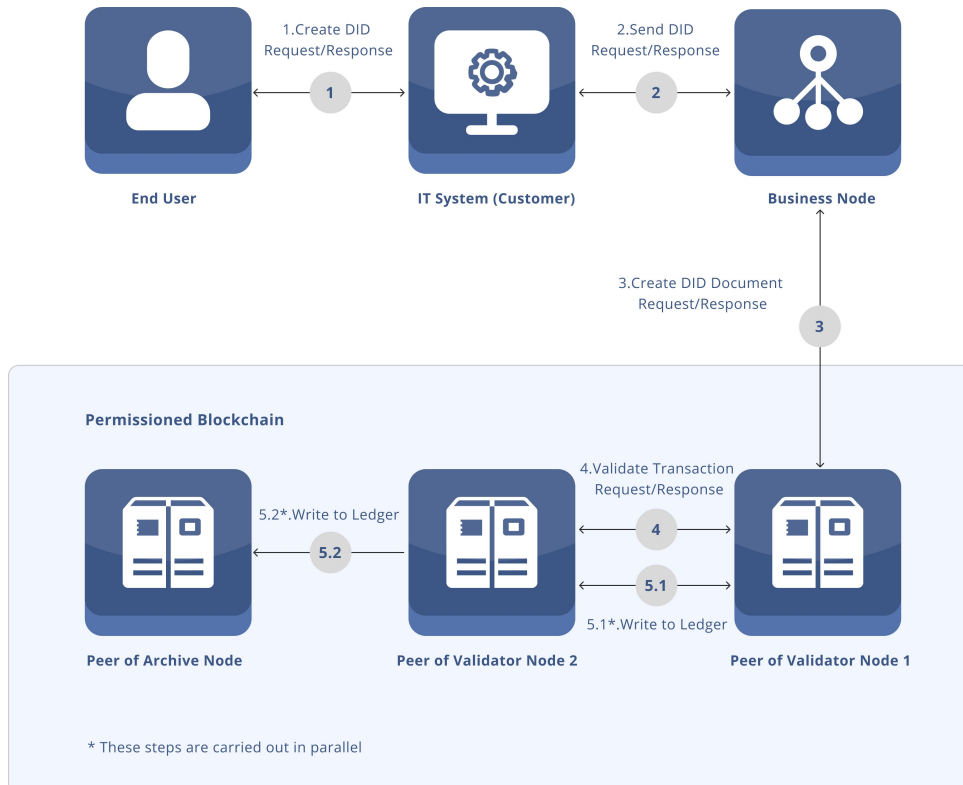
There are four main types of transactions that can be conducted on the UDPN network:

1. Creation of UDPN decentralised IDs (DID)
2. Linking/delinking of CBDC and stablecoin wallets with the DIDs
3. Execution of digital currency transfers & swaps (FX)
4. Providing refunds in case of failed cross-currency swaps (FX)

As the UDPN evolves, more services and operations can be added.

3.1. CREATION OF UDPN DIDs

Figure 9



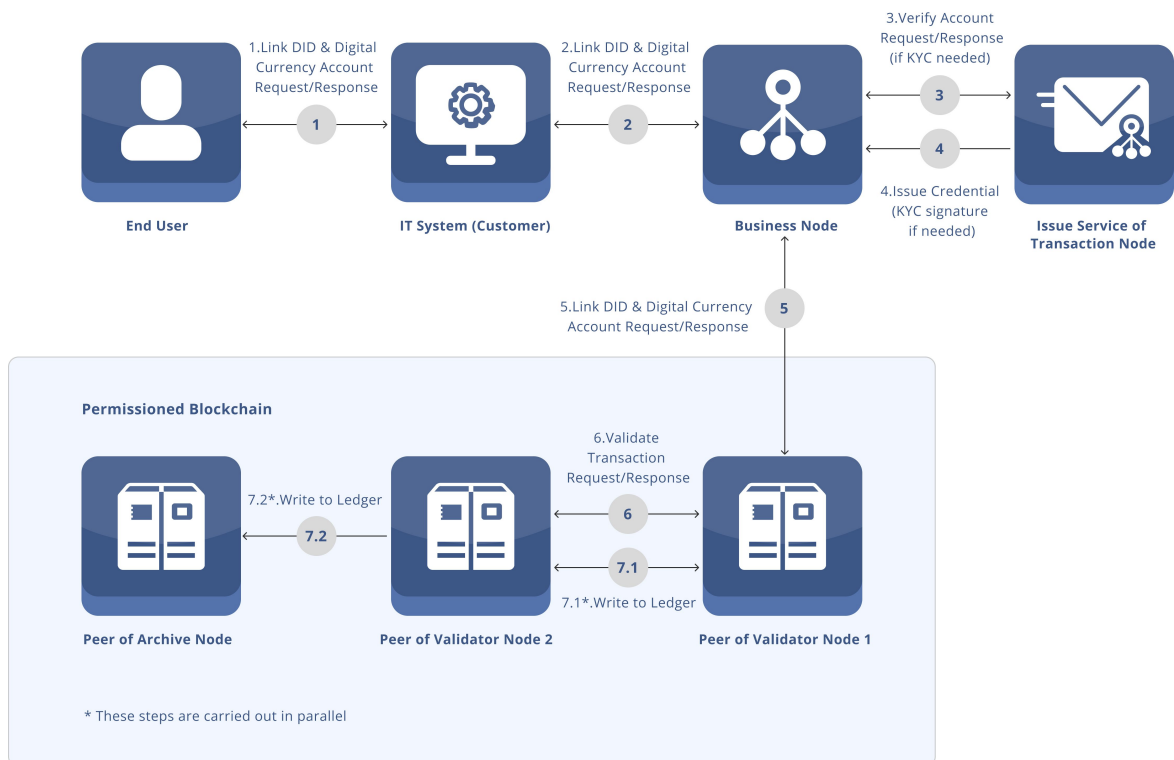
To make any payments using the UDPN, all users must first create a UDPN DID unique to that end user (or business). To initiate the DID creation process, the end user must submit a DID request through the off-chain IT system of the UDPN customer. After the IT system has generated and processed the DID Private Key, it will submit a DID creation request to the Business Node gateway. The Business Node then generates a DID document and submits it to randomly assigned Validator Nodes on the permissioned network.

The Validator Nodes will subsequently validate the DID creation request and write it into the ledger. Each Validator Node will subsequently sync on-chain, first with its peers and then with the TAR Nodes using IBFT 2.0 consensus. The DID creation response is sent back to the Business Node and relayed to the end user via the IT system.

The UDPN provides IT systems with the flexibility to either create a DID for every end user, or to use a single DID and build a user layer on top. In the case where IT systems build a user layer instead of creating individual DIDs for each user, all users can effectively use this single DID for all transactions. If users prefer to own their private keys, Business Node owners can let them generate private keys on their own. Business Node owners will decide themselves which model to use depending on their own business use cases and requirements. The DID documents are maintained on-chain, enabling end users to use the same DID on different Business Node-related systems. DIDs do not contain any personal information.

3.2. LINKING/DE-LINKING DIGITAL CURRENCY ACCOUNTS TO UDPN DIDs

Figure 10




After a UDPN DID has been created, the end user can link their DID with their digital currency accounts or wallets. The process is initiated through a user request to link the DID with a particular digital currency account or wallet through a business IT system. The IT system will subsequently transfer this user's account information, requested by the currency system, along with their KYC details, when needed, via a linking request to the Business Node.

At this stage, the Business Node will submit an account verification request to the Issuer Service of the Transaction Node through an encrypted connection. This will include a KYC check, should the digital currency in question require one. Once verified, the Business Node will subsequently submit a linking request to a Validator Node.

The Validator Nodes will then validate the account linking request and write it onto the ledger. Each Validator Node will subsequently sync on-chain with other Validator Nodes and with the TAR Nodes. The account linking response is sent back to the Business Node and relayed to the end user via the IT system.

A Transaction Node will issue verifiable user credentials (per the W3C Verifiable Credentials Data Model 1.0¹⁰) after successfully verifying the end user's DID and account details. These credentials are signed with the respective Transaction Node's DID and sent via a secure encrypted protocol. Depending on the verification requirements for each currency system, users can link multiple CBDC and stablecoin accounts to a single UDPN DID. The customer has full control over their account credentials, stored locally or in the Business Node's encrypted private storage. Third parties need to be authorised by the customers to access their account credentials.

The delinking process is straightforward. Like the linking process, a delinking request should be submitted by the end users via the IT Systems, who will pass it to the Business Node. The Business Node will then submit a delinking request to the Validator Node, which will process the request on-chain and record it onto the ledger. Once the account credentials are deleted, the currency account is delinked from the DID, and the user cannot conduct any transactions using their DID unless the user performs the linking process again.

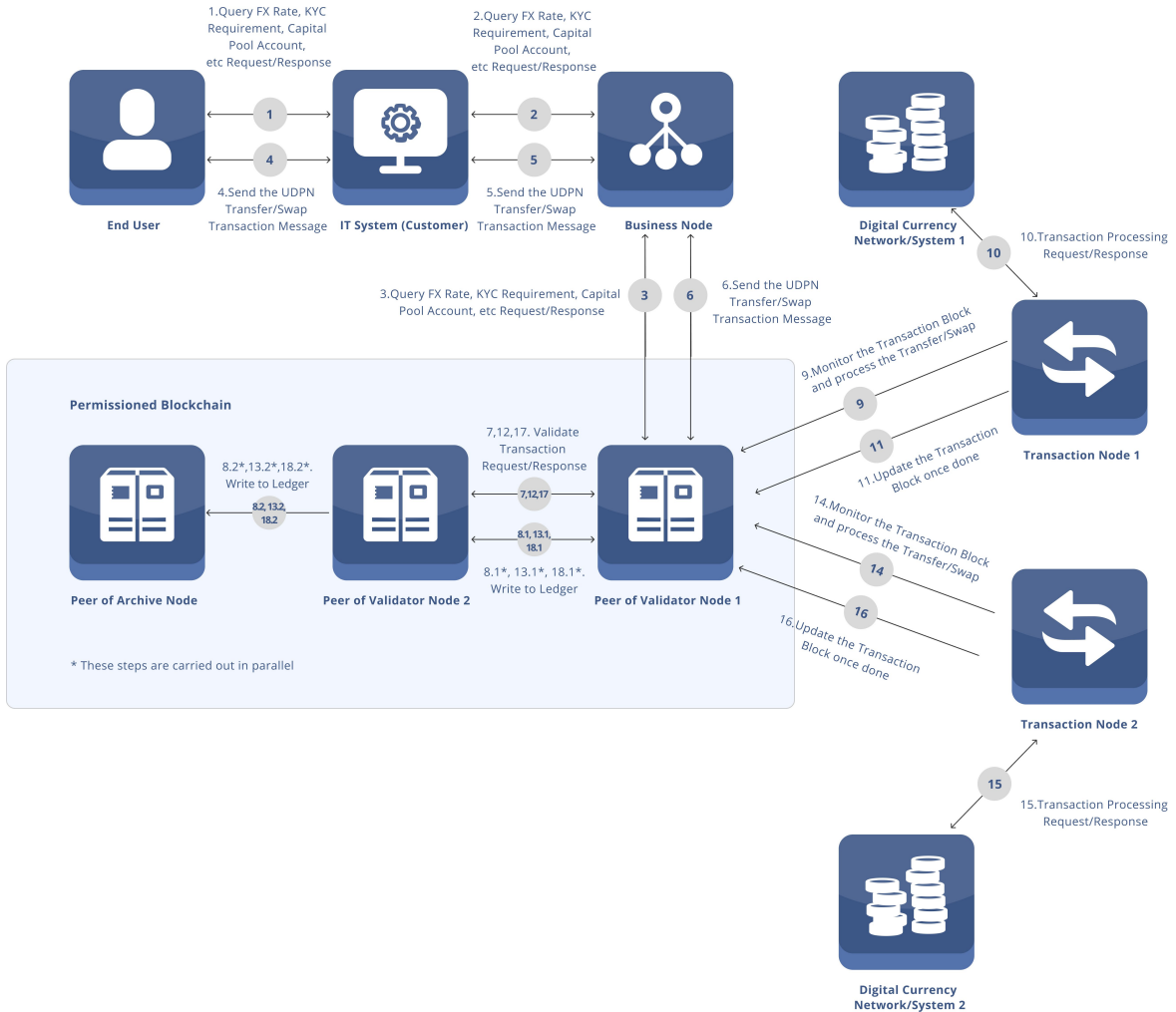


AFTER A UDPN DID HAS BEEN CREATED, THE END USER CAN LINK THEIR DID WITH THEIR DIGITAL CURRENCY ACCOUNTS OR WALLETS.

¹⁰<https://www.w3.org/TR/vc-data-model/#what-is-a-verifiable-credential>

3.3. DIGITAL CURRENCY TRANSFERS & SWAPS (FX)

Figure 11



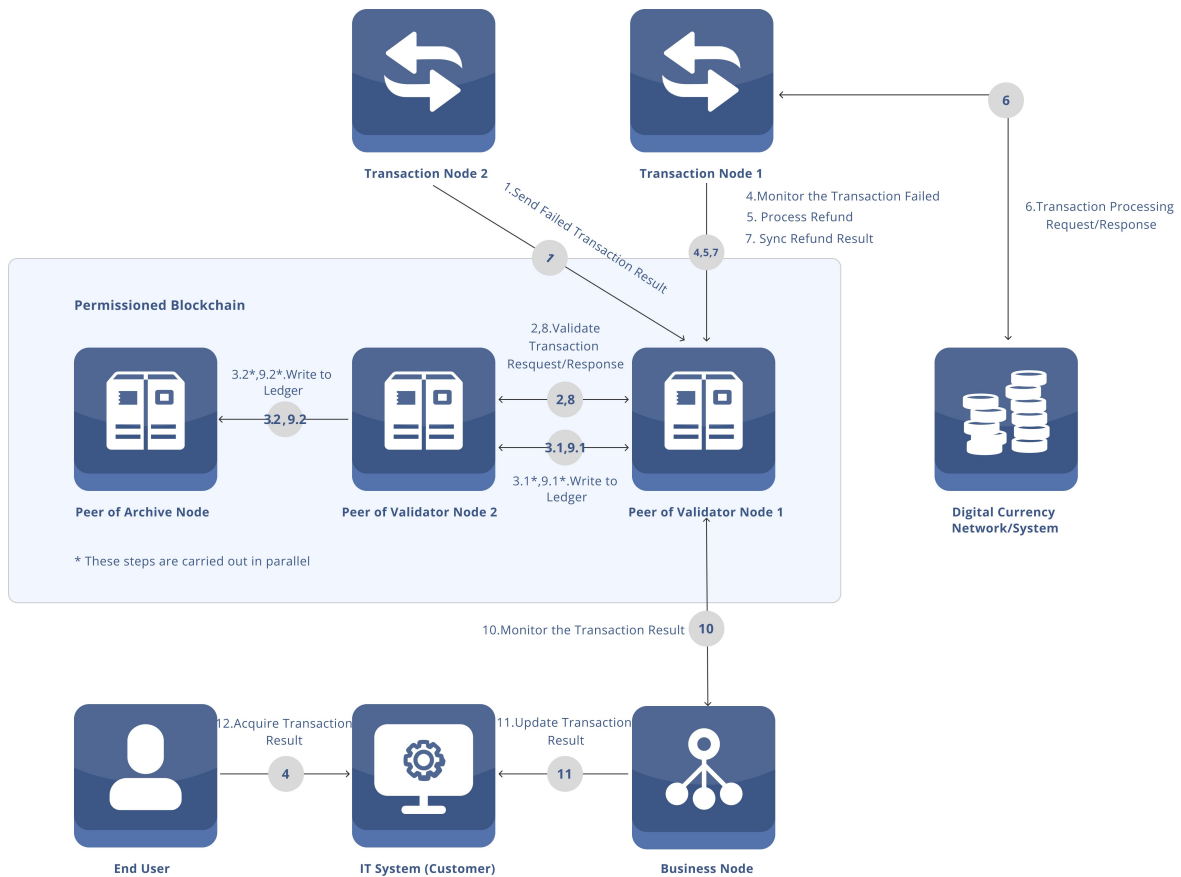
When a transfer or a swap is initiated via the UDPN, the IT system will collect the required transaction information from the end user, including Sender DID, Currency Type, Amount, Sender Account (optional), Receiver DID/Receiver Account, Receiver Currency Type, etc. Subsequently, the IT systems send the transaction requests to Business Nodes via the gateways.

The Business Node compiles the messages based on their respective currencies, and each message is then passed onto the Validator Nodes. During this transmission, the Transaction Node monitors the swap, verifies the sender signatures (or KYC and credentials if required), and processes the transfer or swap by submitting the transaction request to the respective digital currency systems. It must be noted that both transfers and swaps use the same set of smart contracts to execute the requests from the end users. If the currency types in the transaction requests are different, swap processes are initialised.

The currency swap process consists of two transfer processes involving the capital pools of the corresponding currencies. Let us take for instance a 100 digital euro (sender) to digital US dollar (receiver) swap. Whenever a currency exchange is initiated, the UDPN receives a transfer request message from the sender's IT system via a Business Node. The sender's 100 digital Euros is debited from the user's wallet into the Euro capital pool. Subsequently, the message is sent to a corresponding digital dollar Transaction Node, via Validator Nodes, at the selected FX rates. The Euro and digital dollar Transaction Nodes will settle, after which the digital dollar capital pool will deposit the equivalent of 100 digital Euros in digital dollars into the receiver's digital dollar account, thus completing the swap. Running a Validator Node entitles the owner to earn network fees, set via Alliance member vote and evenly divided. FX rates are maintained in real-time via an order-matching system operated by third parties, or alternatively Transaction Nodes can set their own.

3.4. REFUND PROCESS IN THE CASE OF A FAILED TRANSFER

Figure 12



In instances where the system fails to transfer the receiver's currency from the respective capital pool to the receiver's account, a refund is initiated. In the above instance of a swap between digital Euros and digital dollars, the digital euro Transaction Node connected to a digital Euro system will be monitoring the failed transaction on-chain and will send a refund request to the digital Euro system and return the 100 digital euros to the sender's account. Subsequently, the Transaction Node will submit the refund result for validation. Once this is validated and the blocks are written onto the ledger, the Business Node will receive the refund message and update the transaction request to the IT system for the end user.

There is no refund, per se, for same-currency transfers. For refunds in a same-currency transfer, the receiver must make a new payment transaction to the original sender.

4. WHOLESALE DIGITAL CURRENCY SETTLEMENT

When a business wants to initiate a swap transaction from one CBDC to another, the commercial banks operating the Transaction Nodes need to have associated capital pool accounts with the relevant central banks and they must be sure there is adequate capital within those pools.

For example, let us consider an instance where an end user wants to convert digital dollars into digital euros. To process such FX transactions, the digital dollar is transferred from the sender account to the digital dollar capital pool held by 'Commercial Bank A'. Subsequently, an equivalent number of digital euros are transferred from the capital pool held by 'Commercial Bank B' to the user's digital euro account. The FX rate for the transfer will be based on real-time exchange rates sourced from one or more third-party sources and synced to the UDPN network.

'Commercial Bank A', that now holds the digital dollar received from the user, will use a third-party wholesale digital currency settlement system to settle with 'Commercial Bank B', who made the digital euros pay-out to the user. The commercial banks will need to be enrolled with the respective wholesale digital currency settlement systems to easily achieve the settlement between the capital pools.

Over the last few years, we have seen financial services firms across the globe invest considerable resources into improving wholesale use cases for digital payments. Examples of such projects include the creation of BIS m-CBDC bridge¹¹ and Utility Settlement Coin by Fnlity¹². We have also witnessed central banks collaborating on cross-border payment projects as illustrated by Project Dunbar, led by the Monetary Authority of Singapore and the Bank for International Settlements, as well as the m-CBDC Bridge project, jointly led by the Hong Kong Monetary Authority, the Bank of Thailand, the People's Bank of China, the UAE Central Bank, along with the Bank for International Settlements (BIS). The UDPN will work with such projects to integrate wholesale digital currency systems to allow capital pools in different currencies on UDPN settle with each other seamlessly.

¹¹<https://www.finextra.com/newsarticle/33921/big-banks-create-utility-settlement-coin-company>

¹²https://www.bis.org/about/bisih/topics/cbdc/mcbdc_bridge.html

5. SECURITY AND PRIVACY

In a world where cybersecurity attacks on financial networks are increasing, centralised hub-and-spoke models are particularly vulnerable. Security is paramount for all organisations joining the network. Moreover, the UDPN Alliance understands that AML, CFT, financial sanctions, and the prevention of illicit activities at a network level are front of mind for compliance and risk departments within financial institutions. To ensure that the UDPN adheres to the highest possible standards, security frameworks such as ISO 2700X series and NIST are being used as a reference. One of the main objectives of the UDPN is to guarantee security “CIA triad” ensuring Confidentiality, Integrity and Availability of data. The network will be designed so that data is kept confidential and data privacy is guaranteed at all times (in transit, in use and at rest) by using encryption managed by the parties that are taking part in transactions on the network (Business Nodes, Transaction Nodes, etc.) It will implement the mechanisms necessary to guarantee that the data is not corrupted or tampered with, whilst guaranteeing data integrity. Lastly, the UDPN will ensure high system availability and resiliency with proper mechanisms to backup and restore data as part of BCM (Business Continuity Management). This ensures data availability requirements are fulfilled at all times.

5.1. IT SECURITY

The following are the key elements of the network & IT security, which use the CIA principles to ensure robust security across the UDPN network:

- **Security via a DevSecOps approach:** The UDPN will need to define, implement, and improve its own System Development Lifecycle (SDLC) in order to integrate security testing and automation into the software development lifecycle and everyday operations. This will ensure that when any code is developed, it is done to the highest security standards and that when operations are completed, it is in a safe and secure manner. In this regard, a DevSecOps approach is recommended, as it is aligned with the mindset of “agile methodologies”, with security testing being automated and integrated into the process and part of a continuous improvement loop. The UDPN code will be open source and all UDPN Alliance members’ IT security teams (which include some of the best in the world, due to the security needs of financial institutions) and the global security tech community will be encouraged to review and provide feedback on possible security flaws, should any exist.
- **Security in layers:** The UDPN is a decentralised system with a large diversity of roles: businesses (owning “Business Nodes”), regulated financial entities (owning “Transaction Nodes”) and Alliance members (owning “Validator Nodes”). It can therefore be considered a supply chain, in terms of security, with every party involved providing its own infrastructure and individually managing IT security of the nodes for which it is responsible.

The UDPN will establish a security governance mechanism that ensures the security

of the whole system, whilst providing technical standards to all participants. The foundation of this will be the multi-layer Security Operations Centre, which will set and govern the appropriate security requirements for each party. A dedicated CERT/CSIRT will be set up for every party (depending on its role) and have a team responsible for coordinated Security Emergencies and Incident Responses. This will be underpinned by a robust Business Continuity Management (BCM) plan, including Contingency Planning and Disaster Recovery Planning.

- **Zero Trust Model:** In order to guarantee the appropriate management of IT security and assure the implementation of the necessary security measures in production, the UDPN will deploy a Zero Trust Model. Under such a model, no part of the system is considered a “safe area” and every care is taken to protect against both external attackers and malicious insiders. This involves establishing secure communication between components (including nodes), ensuring robust authentication & authorisation between components, creation of a strong proof of identity, establishing the use of physical perimeters and, lastly, having robust protection against any malicious insider activity.
- **Security & Identity Governance:** A strong governance system will minimise and eliminate security concerns that may arise at any level of the network. It will also ensure adherence to compliance and regulatory measures. In place from the outset, at the start of the design phase, the governance system covers everything ranging from the governance requirements for technical standards and compliance, policies for secure operation of the network to a robust governance system for identity issuance.

When it comes to Identity Governance, Public Key Infrastructure (PKI) for node identity provisioning will be implemented and governed by the UDPN Alliance. The Alliance will strive to uphold PKI best practices and implement a secure process for issuing and revoking certificates.

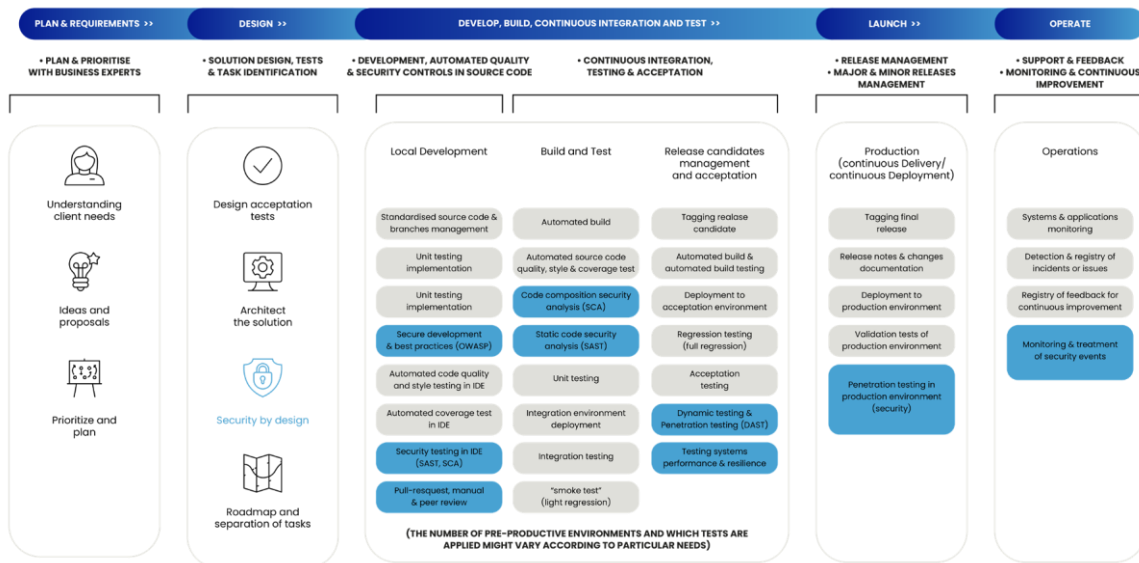
Additionally, to ensure end-to-end security, the UDPN will cover the following areas:

- **Security by design** to enhance the design and fully resilient network and local architectures for all areas
- **Secure development and test best practices** are fulfilled by all developers working on the project
- **SAST (Static Application Static Testing)** both in “local development” and “build and test” phases. SAST testing consists of scanning source code and/or binaries to detect vulnerabilities in all areas of the individual components and the overall network.
- **SCA (Software Composition Analysis)** whereby libraries/dependencies used by the UDPN source code are scanned for vulnerabilities on a regular basis.
- **DAST (Dynamic application testing and penetration testing)** to target vulnerabilities in the runtime environment. The UDPN applies dynamic testing in both low-level environments as well as in production.
- **Performance and resilience of testing systems** will be frequently validated by the UDPN in order to guarantee that the system is available, working well under the desired/ estimated load conditions and remains resilient when faced with unexpected situations (such as a sudden surge in swap transactions after a new

currency comes online). One of the main goals is to boost system readiness for business continuity. An SRE (Site Reliability Engineering) testing approach, such as Chaos Engineering, will be used.

- **IT Security in production** will include security observability, response to security incidents and Business Continuity Management.

Figure 13



In the past, the industry has witnessed attacks on systems, known as supply chain security attacks. Some of these infamous attacks succeeded because of vulnerabilities in the supply chain. The fact that a security issue from one of the parties can affect (to a major or minor degree) other related parties is a reality for which the UDPN network is well prepared. In order to mitigate such risks, the UDPN will define clear terms of security management when integrating new participants and automate risk flags to show whether participants are using the correct security procedures (for example, the encryption of local data). A UDPN Technical Standard, describing the security requirements and procedures that every party needs to fulfil according to their role in the UDPN Alliance, will be created to define the aforementioned standards and procedures.

5.2. NETWORK SECURITY

Security is critical for all organisations joining the network. The UDPN Alliance understands AML, CFT, financial sanctions, and the prevention of illicit activities are front of mind for Compliance officers and related departments within any financial institution. The UDPN design is regulator-friendly, with regulators and auditors having access to TAR Nodes, which facilitate access to all transaction data.

The following areas of network security will be taken into consideration:

- **Funds handling on the network:** The UDPN Alliance and the network itself will never hold customers' or users' funds. Transaction Nodes can only be operated by regulated and licensed local money service providers and banks.
- **Compliance Framework:** The UDPN Alliance will meet all of its compliance obligations by ensuring it meets or exceeds the regulatory requirements in the countries and regions it operates. Strict due diligence processes will be implemented for current and new members of the Alliance. This is to ensure the network is used to facilitate financial inclusion and the compliant exchange of value rather than contributing towards financial terrorism and money laundering. Alliance members will also work together to ensure proper programs exist to address current AML/CFT regulations and financial sanctions to create a secure environment for conducting cross-border exchanges. Additionally, financial intelligence services will be developed to prevent illegal payment activities.
- **Financial Intelligence Services & Relationship Management:** As regulators pay greater attention to compliance and regulatory issues in the digital assets markets, it is critical for financial institutions providing digital currency services to understand with whom they do business and to have proper access to their counterparties' compliance and fraud details. Such information will be available on the UDPN in the form of the aforementioned financial intelligence services, provided through the TAR nodes. At launch, UDPN users will be able to define which financial institutions they desire to do business with and deny messages from non-trusted financial institutions. Such features do not currently exist for stablecoin transfers on public chains, as these systems are permissionless by design and so create significant fraud/KYC risks for any financial institution expanding their stablecoin services offering. These financial intelligence services features will be available within the Transaction Node.
- **Due Diligence Approach:** UDPN members (Alliance and Transaction Nodes especially) are leaders in their respective industries and will need to adhere to the highest business standards. To protect client relationships and the reputation of its members, the UDPN Alliance will implement strict screening processes that will include a thorough review of prospective new Members. These due diligence reviews will be completed for all new members on an ongoing basis to ensure the network is composed of organisations upholding the highest business and compliance standards.
- **Regulatory Considerations: The "Travel Rule":** The UDPN Alliance will also ensure that the network facilitates the convenient cross-border exchange of value, whilst providing the necessary infrastructure for network users to comply with their regulatory obligations, including the Travel Rule brought in by FATF. This rule states that all financial institutions should provide certain customer information to the corresponding financial institutions when the transfer amount exceeds a certain threshold as well as when the transfer involves more than one financial institution.

As a decentralised permissioned blockchain network, the UDPN will interface with IT systems and digital currency issuers & holders via encrypted and secure APIs. Moreover, the UDPN DID will be certificate controlled, with two layers of certification,

providing more security to the transactions on the network. All off-chain data sources will interact with the permissioned decentralised network via secure and digitally signed connections.

5.3. PRIVACY

As a messaging platform, the UDPN does not store any user information, with most of the user's personal and privacy data being stored off-chain within the business IT systems. All interactions between the end users and business IT systems are conducted off-chain and do not occur on the UDPN. For transactions that take place on the UDPN, only the Validator Nodes and TAR Nodes will be able to view certain details of a transaction request (in those instances without end user personal information). The Business Nodes and Transaction Nodes store their non-transactional data off-chain and have access to some KYC information where the currency system requires KYC checks.

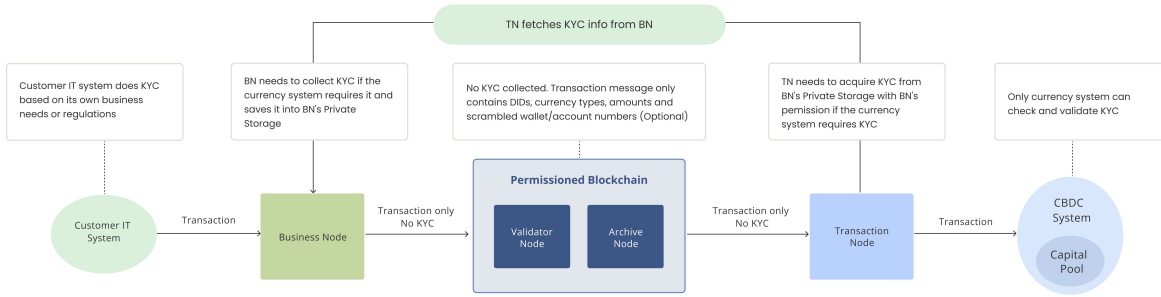
Given that end users do not connect directly with the UDPN, but rather through third-party IT systems, all personal data is stored and held by third-party businesses and not by the UDPN. The on-chain DID is always anonymous, with all KYC and credentials being stored in private storage held on Business Nodes. The assigned Validator Node is only able to validate the message format and whether the message originates from a certified Business Node. They can verify the presence of DID information, without having access to personally identifiable information. The message also includes information about the transfer amount, currency types, account IDs and scrambled wallet addresses. All end users' CBDC wallet IDs and account numbers are anonymised when the message is sent to the Validator Nodes. Therefore, the privacy of the end user is protected at all times.

After a message is sent from the Validator Node, the receiving Transaction Node will only decrypt the required information to ensure compliance with applicable payment laws and regulations. Finally, it is worth noting that the data stored on the Archive Nodes is only accessible to regulators, central banks and auditors, for AML/CFT monitoring and auditing purposes.

**AS A MESSAGING
PLATFORM, THE UDPN
DOES NOT STORE ANY
USER INFORMATION, WITH
MOST OF THE USER'S
PERSONAL AND PRIVACY
DATA BEING STORED
OFF-CHAIN WITHIN THE
BUSINESS IT SYSTEM.**

5.4. KNOW YOUR CUSTOMER (KYC) RULES

Figure 14



Note: If the currency system doesn't require KYC, such as public chain-based stablecoins, no KYC will be processed on UDPN

Note: If the currency system doesn't require KYC, such as public chain-based stablecoins, no KYC will be processed on UDPN

The fundamental nature of the UDPN network is that of a messaging service for digital currency transactions. Decisions regarding the legality of transactions rest with the IT systems onboarding end users and/ or currency systems. Those businesses providing end users access to the UDPN and those financial institutions operating Transaction Nodes need to ensure that transactions comply with relevant local and international regulations and with the currency system requirements. Failure to comply with the relevant rules may result in the institutions facing potential sanctions and fines imposed by their respective regulatory authorities.

When an end user wants to use the UDPN network, it must first go through an onboarding process with the respective business IT system. The IT system may need to conduct the KYC as per their business requirements or local regulations. When a transaction is initiated, the transaction request is sent from the IT system to the Business Node and subsequently to the Validator Node. This transaction message only contains DIDs, currency types, amounts and scrambled wallet/account numbers (optional). When the transaction reaches the Transaction Node, the scrambled account numbers will be decrypted and the transaction is then submitted to the currency system along with KYC information if required.

If the currency system doesn't require KYC, for example as with public chain-based stablecoins, no KYC will be processed on the UDPN and the transaction will go through the value chain without any KYC. In those instances where the currency systems do require KYC, the Business Node will collect the required KYC data from the IT systems and save it into the Business Node's private storage. The amount of KYC information provided by the Business Node is dependent on the requirements of the respective currency system. The Transaction Node fetches the encrypted KYC information from the Business Node and subsequently passes it on to the currency system. The currency system decrypts the KYC information and validates whether the user satisfies the requirement, before completing the transaction.

In the case of a swap between two currencies, if the receiving currency system requires the sender's KYC, the UDPN would require the Business Node to also authorise the receiving currency's Transaction Node to access the KYC. The KYC requirements of the Transaction Node need to match the KYC available from the Business Node. Where appropriate KYC data is unavailable to the receiving Transaction Node, the transaction would not be processed.

6. REGULATORY COMPLIANCE

The UDPN Alliance is deeply committed to adhering to the highest compliance standards and will ensure that it meets or exceeds the regulatory requirements of the countries and regions in which it operates. Strict due diligence processes will be implemented for current and new members of the Alliance, to ensure that the network is used as a tool to facilitate financial inclusion and the compliant exchange of value, whilst prohibiting any financial terrorism and money laundering.

The UDPN Alliance and the network itself will never hold or move funds. Additionally, the Transaction Nodes can only be operated by regulated and licensed local money service providers and banks. Working in conjunction with global authorities the UDPN Alliance members will create a secure environment for conducting cross-border exchanges and ensure that AML and CFT risks are managed, sanctions requirements are met, and all regulatory requirements are adhered to.

Given that the majority of Transaction Node owners are commercial banks, they are obliged to follow the strict compliance and regulatory requirements of the currency systems to which they connect. Business Node owners are required to provide the UDPN with their relevant KYC information. In addition, the UDPN will apply a “regional code” to every Business Node, based on its country and region. The UDPN will only allow Business Nodes to access currencies and enable transactions so far as is permissible in accordance with the relevant country’s laws and regulations.

Similar to SWIFT, the UDPN does not exert any control over the messages sent by Business Node owners over the network. Validating the authenticity of messages, and any related KYC information, remains the responsibility of the individual currency systems. As such, the currency systems themselves remain responsible for sanctions related screening and reporting, as well as for the application of any locally applicable laws and regulations. The nature of the digital currency messaging systems means that the network cannot itself administrate such screening and reporting, but instead works to facilitate the ease with which its users meet their own responsibilities in relation to national and international regulations.

7. UDPN ALLIANCE & GOVERNANCE

7.1. ORGANISATION & FOUNDING MEMBERS

The UDPN Alliance's primary purpose is to improve the efficiency of digital currency payments through the creation of a shared decentralised network complete with associated standards. The UDPN provides a secure network that operates in accordance with local laws and regulations, through which any enterprise from around the world can perform payment transactions and settlements, in various digital currencies, simply by accessing their local Business Nodes. In order to achieve this, the Alliance will partner with best-in-class FinTech providers, institutional finance partners, and digital finance experts to rapidly accelerate the development, deployment, commercialisation, and global scaling of the UDPN ecosystem.

The goal is to have eight founding Alliance members acting as the initiators of the UDPN. The Alliance members are a diverse collection of organisations representing various verticals of the ecosystem from technology firms and multinational banks to central banks and major payment providers. This core group forms the nucleus for an international alliance that is responsible for developing the roadmap, standards, governance, and commercialisation strategy for the UDPN. Each founding Alliance member has equal rights and is selected in such a way as to provide cross-geographical representation. The partners voluntarily invest resources into the UDPN, with core members conducting activities in a coordinated fashion. Any applicable income derived from the UDPN infrastructure will be equally shared between the UDPN Alliance members.

This decentralised governance structure ensures that no single party will be able to gain full control of the UDPN, and the UDPN always remains a neutral platform with equal rights for all members. All decisions are taken after voting by members, with appropriate voting thresholds set for different types of decision. The UDPN will establish a governing council, with each member having one representative. All members will take turns to chair this council on a quarterly basis. There is no controlling entity, CEO or board of directors for the UDPN. This ensures that no single person, entity, organisation or sovereign government can take control of the network.

Being an advocate of an open-source ecosystem, the Alliance will keep the Validator Nodes and Business Nodes open-sourced. Additionally, the Alliance members will ensure that UDPN developments remain within one single codebase. All member stakeholders will have access to the codebase and any related documentation at any given time, including during the development phases.

7.2. DECENTRALISED GOVERNANCE AND VOTING

The UDPN is jointly managed and governed by all Validator Node owners through a distributed governance framework.. Each Validator Node owner is expected to

participate in the decision-making process of the Alliance and each Validator Node owner has one vote to cast. Matters relating to the development, maintenance and operation of the UDPN are determined by this voting process. To ensure robust governance, the voting process will require either one vote, simple majority or a super majority of 80% to approve decisions regarding the UDPN, with different thresholds applied depending on the topic. The list of voting categories is below. Most items will only be executed by a majority or supermajority vote from all Alliance members.

INSTANCES WHERE VOTING IS REQUIRED:

1. Establishment of new Validator Nodes
2. Establishment of Business Nodes
3. Establishment of Transaction Nodes
4. Matters related to the upgrade of UDPN node software
5. Matters related to the upgrade and deployment of smart contracts
6. Deciding upon the fee structure for currency transfers and swaps (FX)
7. Deciding upon the revenue share model
8. Deployment of new services on the UDPN

A distributed governance system is deployed by UDPN Alliance members. Under this system Validator Node owners have the right to vote on various decisions relating to the UDPN's operations. This includes the UDPN roadmap, standards, governance, commercialisation strategy, management of payment operations and network monitoring. Important tasks on the UDPN, such as the addition of new nodes to the network or smart contract updates, can only be executed following an approval vote by the UDPN Alliance members.

7.3. REVENUE MODEL

In the initial stages, the UDPN will not charge users, thus allowing more users to experience the platform and overcome any friction. Following the initial phase, the UDPN's primary revenue streams will be derived from the fees generated by swaps and transfers, which will be automatically charged on the system to users of the UDPN. The revenue will be equally shared among Alliance partners, with proceeds being periodically distributed to the UDPN Alliance members directly via on-chain smart contracts. A large proportion of the revenue generated will also be invested into the ongoing development and maintenance of the UDPN.

8. SOCIAL IMPACT

The UDPN is positioned as a global payment infrastructure. The main driver of this positioning stems from the desire to bring accessible and easy cross-border payment capability to those people who currently have limited or no access to straightforward digital payments. This sentiment is echoed by many CBDC projects, which often focus on increasing financial inclusion and significantly lowering costs, all while improving accessibility.

In many emerging economies people and businesses lack access to banking services, hindering economic and social development. Those who do have access to banking services often face high transaction and account fees, coupled with slow transfer times and limited transparency. The UDPN Alliance wants to tackle this issue and increase financial inclusion. It is keen to collaborate with institutions that are also committed to solving these issues and that can build user-friendly front-end payment services with UDPN access.

9. ROADMAP

The UDPN is being built for both the present and the future. CBDCs and stablecoins are anticipated to become an integral part of the cross-border payment ecosystem. The UDPN is ideally placed to be the primary choice for central banks when it comes to the distribution of their own digital currencies. The same is true for enterprise IT systems looking to access all digital currencies with one single infrastructure. With the UDPN, the evolving payments ecosystem can move towards a vastly improved and more resilient future, one which is in sync with emerging technologies. Key to the UDPN's success will be the ongoing and continuous integration of all relevant CBDCs and stablecoins.

The Alliance will add to its eight founding members, growing gradually to 24 over the next two years, each running their own Validator Node. The additional 16 members will include a diverse representation of central banks, commercial banks and technology companies. Focusing initially on a handful of major regulated stablecoin currency systems, the Alliance members aim to have over 100 currencies on the UDPN in a few years, making it a powerful network for all stakeholders.

Although central banks globally are advancing their engagement with CBDCs, barring a few exceptions, most have just started progressing from discussion stages to experimentation. With most CBDCs in the early stages of development, it is anticipated that the digital currency cross-border payments ecosystem will be driven by the rise of stablecoins in the next couple of years. This provides the UDPN sufficient time in which to establish a robust foundation, so as to be the go-to platform for all central banks, as and when they launch their CBDCs.

In line with these expectations, the beta release of the UDPN is scheduled to go live with 2 to 5 stablecoins in Q4 2022, with pilot commercialisation by mid-2023. Subsequently, full-scale global deployment will be targeted within two years, incorporating stablecoins and eventually CBDCs.

The UDPN is positioned to become the global messaging backbone, connecting all CBDCs and stablecoins. Furthermore, its design and architecture also support connections to traditional account systems, such as commercial bank accounts and payment service accounts. Therefore, the UDPN can also potentially act as a bridge between digital currency accounts and traditional bank accounts.

10. CONCLUSION

Digital currencies are changing the world as we know it, with a seismic shift being felt across the financial sector. Driven by the need to promote financial inclusion, increase competition and fix broken payment infrastructure, each central bank will have to restructure their banking systems over the next decade.

Distributed Ledger Technologies enable end-to-end transparency for central banks when circulating their digital currencies. They significantly increase the efficiency of monetary policy, whilst mitigating the risk of failure and also significantly reduce transaction costs. They also enable central banks to pay benefits, grants and stimulus funds directly to individuals, especially those who are unbanked, or underbanked. With CBDCs, end users can potentially have full control of their money through a direct account with the central bank and may not necessarily be required to hold their deposits with a traditional commercial bank.

With multiple CBDCs being created on different underlying technology protocols, the UDPN is critical for interoperability and provides a secure messaging platform, fit for this new money economy. Through the UDPN, multiple CBDCs and stablecoins can be easily integrated for seamless and fast cross-border payments, globally.

The technologies underpinning the decentralised financial system are constantly evolving, with rapid improvements taking place on a regular basis. These pioneering technologies are revolutionary for financial services, and the UDPN is exploring how best to improve people's lives and contribute to the industry. Continued innovation and competition will be key to driving increased efficiency and lowering costs and the UDPN plans to be an important part of this landscape.

Financial institutions are approaching a critical turning point in the evolution of the global financial system. Rapid changes in technology are driving significant alterations to the business models of financial institutions, which are adapting to meet the changing needs of their customers and to ensure their long-term profitability and viability. Banks are essential participants in the UDPN, engaging with their relevant central banks, providing capital pools and providing the liquidity necessary for cross-border transactions. In turn, engagement with the UDPN provides financial institutions with an opportunity to actively participate in the evolution of the financial ecosystem.

The UDPN's ethos centres around collaboration and its objective of improved inclusivity underpins its design for the infrastructure of the future. The next steps for the UDPN will be to focus on testing the network's full capabilities, proving the robustness and security of the systems. The UDPN's influence and impact on the furthering of decentralised finance and the digital economy will continue to grow as more regulated digital currencies are added and additional Alliance members join.

The UDPN Alliance would like to invite like-minded institutions and experts to collaborate with us and be part of this transformational moment in financial history. No system is perfect, and as the UDPN is scaled up in this complex world of fast-evolving technology and strict and varying regulatory environments, there are bound to be areas in which the network can be improved. The Alliance is a collaborative body that endeavours to learn from global experts in order to continually improve the UDPN system. This will ensure its place as the world's principal digital currency payment messaging network.

Please reach out to the Alliance to contribute to our mission to build an inclusive, low-cost, fast and easily accessible global payments ecosystem.

