Telco Stablecoin Development
Version 1.0
17 March 2025

*This is a **whitepaper** of the GSMA*

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Antitrust Notice

1 Executive Summary

The telecommunications sector can benefit from stablecoin adoption, as they can streamline cross-border payments by reducing costs, increasing transparency, accelerating processing times, both within the industry and across the digital payments ecosystem.

But the integration of a stablecoin into the telecom industry as a new digital payment method is not without its complexities and challenges.

This document provides an analysis of how a stablecoin arrangement can be introduced specifically within the telco industry, and it seeks to explore organizational, financial, legal (regulatory), and technical dimensions involved in creating a stablecoin solution for the telecommunications market.

The main challenges which require a deep analysis and understanding before any decision about the design and implementation of a stablecoin arrangement can be made include:

- The current lack of regulatory consistency across jurisdictions and its implications on the organizational structure of the stablecoin arrangement
- The contrasting effects and risks of stablecoins on Emerging Markets and Developing Economies (EMDEs) compared to Advanced Economies (AEs)
- The denomination of the stablecoin, i.e., the right choice of the peg currency (or basket of currencies) of the stablecoin since this is a crucial factor for the stability of the stablecoin. This may have important macroeconomic implications for monetary and financial stability if the stablecoin is treated by authorities and regulators as systemically important
- Blockchain/ DLT agility: Blockchain/ DLT systems change rapidly and undergo a process of continuous and accelerated technological development.

The benefits of stablecoins are outlined in the introduction chapter of this paper. In addition to the outlined benefits, a global telecom consortium issuing a stablecoin can harness the power of widespread acceptance. As the stablecoin's acceptance and usage grow, participating telecom enterprises can reap the rewards of network effects and economies of scale. Telecoms should always review the regulatory compliance. As a stablecoin arrangement expands, so too does the responsibility for maintaining and supporting financial stability in collaboration with regulatory bodies and institutions.

One important decision to be made is whether the stablecoin arrangement will serve solely the wholesale market or expand to include retail consumers. This choice significantly impacts various factors, including regulatory compliance, data privacy, security, the setup and scaling of on- and off-ramp entities, as well as wallet accessibility. Generally, the complexities and burdens associated with these areas are higher when the retail market is included.

To tackle the above-mentioned challenges and to start building a robust foundation for a stablecoin arrangement we have outlined in chapter 12.1 (Recommendations) on a high-level basis an approach.

2 Introduction

Stablecoins are digital currencies designed to maintain a stable value by pegging their worth to a reserve asset, such as a fiat currency like the US dollar, a basket of fiat currencies or a commodity like gold. Stablecoins can potentially offer a reliable medium of exchange and store of value within the Distributed Ledger Technology (DLT-World) [1]. In the telecommunications industry, the adoption of stablecoins can bring significant value by enhancing the efficiency, security, and cost-effectiveness of transactions, both within the industry itself and in the broader ecosystem of digital payments and services. By leveraging the potential benefits of stablecoins, telecom companies can streamline cross-border transactions, improve customer payment processes, reduce currency exchange risks, and foster greater financial inclusion for their customers. This introduction sets the stage for exploring the myriad ways in which stablecoins can revolutionize the telecommunications sector and drive innovation in the digital economy.

With the benefits of crypto and additional stability, stablecoins act as a bridge between the old and new financial systems, enabling seamless and low-cost transactions. A transaction of $200 transferred via stablecoin remittance can cost a fraction of a cent, versus the global average charge of $12, (or even up to $30 in some jurisdictions) [2] for transferring traditional cash. With stablecoins, telcos can potentially avoid complexities associated with multiple currency conversions and international wire transfers. Telcos can potentially mitigate currency risk by conducting transactions with stablecoins, ensuring that the value of assets remains more consistent. This stability not only protects against potential losses but also provides a foundation for better financial planning and budgeting.

The telecom industry faces similar challenges for any global inter-partner settlement often involving entities based in different countries i.e., B2B transactions. The industry through the GSM Association has used Special Drawing Rights (SDR) quite successfully as a means for arriving at standardised exchange rates for local currencies in wholesale roaming settlement.

For C2C transactions the industry runs mobile money services [3]. In some business areas like IoT when payment functions are embedded, processing is organized centrally. Centralized control increases the risk of single point of failures and security attacks. It's weak identity mechanisms and higher transaction costs make them a less desirable option.

The advent of blockchain technology brings forth an opportunity to handle a lot of the above challenges through its tokenisation feature, i.e., the ability to associate a value digitally to any object for example collectibles (arts or craft), real estate and shares. Stablecoins present a best of both world scenario and are also seen as a means for mass adoption of the digitized tokens or crypto assets. The established use of SDRs in the telecom industry and likewise use of some stronger currencies has laid the groundwork for a stable telco currency potentially as an electronic SDR or an eSDR [4]. The use of Stablecoins of other established payment currencies like USD or Euro or other basket of stable financial instruments cannot be overruled either.

Potential benefits for telecom industry to adapt stablecoins include:

I. Settlements based on stablecoins could offer cheaper financial transactions – this applies to cross-border settlements - since third parties are eliminated and currency conversion costs are minimized.

II. Stablecoins can potentially offer a stable currency and can help protecting customers in inflationary countries from inflation if the reference asset is a foreign currency.

III. Settlements based on stablecoins with transaction fees of less than a cent could offer micropayment transactions — sub-dollar payments for access to online articles or other small-value digital goods and services.

IV. Stablecoins could potentially leverage interoperability in different areas and dimensions:

   a. Interoperability between applications within an ecosystem (i.e., a large ecosystem of industry-specific applications where payment processes are embedded (i.e. IoT), and settlement is possible between them)

   b. Interoperability between applications cross-ecosystem (i.e., interoperable settlement between industry-specific application ecosystems and 3rd party ecosystems existing on alternative networks (i.e. IoT))

   c. Interoperability with fully digitized international monetary system, means interoperability with national and international Central Bank Digital Currencies (CBDCs)

V. Stablecoins could potentially enable inclusion of “underbanked” people

VI. Stablecoins could potentially enable automated payments in areas like Non Fungible Tokens (NFTs), Real Word Assets (RWAs), dApps or the Metaverse

VII. Stablecoins could potentially enable Decentralized Finance (DeFi) like lending and borrowing platforms, but the industry could provide other financial primitives like lending borrowing and savings. While this business area isn’t a primary focus for telecoms, they can certainly explore this area if they believe it offers strategic value.

VIII. Depending on the design of the stablecoin it could leverage a “related” telco crypto coin and could increase revenue potential if the telco crypto coin market price increases. For example: telco assets such as core network elements could be tokenized for raising capital. Stablecoins can also potentially be used by financial institutions for corporate bonds (for example), providing access to greater liquidity when issuing bonds thanks to a broader market of potential investors.

IX. Use of underlying blockchain technology potentially adds benefits such as transparency, security, and immutability providing proof of record of all the monetary transactions conducted using the agreed stablecoin.

Use of stablecoins could be a problem solver for most of the above-mentioned weaknesses in the B2B, C2C and B2C markets, and the remit of this paper is to explore if and how the above stablecoin benefits can be realised.

2.1 Scope

Below items are in scope of this document

- Types and roles of Stablecoins
- Some jurisdictional legal and regulatory considerations
- Accounting and reporting requirements for a Stablecoin.

- Guidance on management of operational, market, and capital risks of using Stablecoins.
- Overview of stablecoin design patterns, including their pros and cons, and present an economic model for use of carrier based stablecoins in telecom industry and outside.
- Framework for implementation and standardisation work on introduction of stablecoins in telecom industry.
- Outlook of DLT stablecoin integration into current and future ICT services in IOT, Metaverse, roaming etc. serving as a basis for implementation of a potential stablecoin MVP.
- Explore on a high-level basis tokenisation and clearly articulate its differences from a stablecoin. A detailed evaluation of Tokenisation will be done in a separate GSMA document.
- Cybersecurity assessment and best practices recommendations in cyber safety execution
- Recommendations and next steps for stablecoin implementation in the ICT industry.

2.2 Out of scope

Below items are out of scope of this document

- Detail requirements and design of a functional stablecoin system: PoC, MVP or production environment.
- Build a system or specifications for tokenized assets. Any implementation artifacts
- Proposal for a holistic solution for a stable telco coin
- Legal or regulatory advice/guidance

2.3 Organization of this paper

The objective of this paper is to offer coverage of the organizational, financial and technical aspects involved in establishing a stablecoin arrangement for the telecom industry. While a deep dive into detail might not be feasible, we will highlight some important elements.

To remain neutral regarding specific DLT/ blockchain options, this paper focuses on the conceptual level, leaving the technical implementation details open. This approach allows implementers a degree of flexibility, with implementation options being suggested but not elaborated upon in detail.

Unless otherwise and explicitly stated, the statements in all chapters apply to wholesale as well as to the retail market.

This paper shall provide guidance for the various parties involved in a project to introduce stablecoins for the telecom industry. The sections 3-6 remain high-level due to several reasons. First, to help the different stakeholders who partly have limited familiarity with the concepts and impacts of stablecoins, secondly and this is the more important reason, a

cross-border payment system involves several jurisdictions and for every local jurisdiction very different requirements and regulations exist.

In section 3 the characteristics that determine the different types of stablecoins are described as far as they are relevant for a stablecoin arrangement in the telecom industry. It follows the section 4 which refers to some legal and regulatory aspects of using a stablecoin. Section 5 refers to account and reporting requirements for a telecom company, and in section 6 aspects from the risk management perspective are presented.

Section 7 is the main chapter of this paper. It is divided into three parts. Section 7 kicks off with a visionary perspective on how the GSMA could assist the industry to utilize a global stablecoin within the telecom industry. The second part explores different use cases, and the last part covers the main points to build a compliant system.

In section 8 the main aspects and approaches of a DLT architecture are presented and possible DLT/blockchain candidates are selected.

Cyber security and data privacy aspects are part of section 9.

Section 10 outlines where standardization regarding the telecom industry could leverage the use and further evolvement of Stablecoins.

The remainder of the paper (section 11) contains outlooks on how stablecoins can potentially be applied in various telecom specific use cases.

Section 12 provides conclusion.

2.4 Definitions

Term	Description
Blockchain	means a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. Each block in the chain contains a number of transactions, and every time a new transaction occurs on the blockchain, a record of that transaction is added to every participant's ledger. Each block N is containing a reference to a hash of block N-1. Notably, the distribution and duplication of data is a function of consensus, not blockchain
Distributed Ledger Technology (DLT)	refers to the technological infrastructure and protocols that allows simultaneous access, validation, and record updating in an immutable manner across a network that's spread across multiple entities or locations. Some examples of DLT are, Ethereum, Hyperledger Fabric, and Corda.
Electronic Know Your Business	Electronic Know Your Business is a method for corporate identity verification, see KYB
Know your business	Know your business is the process of verifying the ownership and legitimacy of a business before entering a relationship with it.
Mobile Money	A service in which the mobile phone is used to access financial services. Mobile money transfer. A movement of value that is made from a mobile wallet, accrues to a mobile wallet, and/or is initiated using a mobile phone. Mobile payment.

Term	Description
Mobile financial services	The use of a mobile phone to access financial services and execute financial transactions. This includes both transactional and non-transactional services, such as viewing financial information on a user's mobile phone.

2.5 Abbreviations

Term	Description
ACH	Automated Clearing House
API	Application Programming Interface
CBDC	Central Bank Digital Currency See also: https://www.investopedia.com/terms/c/central-bank-digital-currency-cbdc.asp
CASP	Crypto Asset Service Providers
CEX	Centralized Exchange
CDR	Call Detail Record
CFTC	Commodity Futures Trading Commission See also: https://www.investopedia.com/terms/c/cftc.asp
DEFI	DeFi, "Decentralized Finance" See also: https://www.investopedia.com/decentralized-finance-defi-5113835
DEX	Decentralized Exchange
DLT	Distributed Ledger Technology
eKYB	Electronic Know your Business
EOA	Externally Owned Account
EU	European Union
FSA	Financial Service Authority See also: https://www.investopedia.com/terms/f/financial-services-authority-fsa.asp
GDPR	General Data Protection Regulation
GraphQL	GraphQL is a query language to build APIs
GUI	Graphical User Interface
HGB	Handelsgesetzbuch
IFRS	International Financial Reporting Standards
IOT	Internet of things
I(I)oT	Industrial Internet of things
JSON	JavaScript Object Notation
KYB	Know your business
MAS	The Monetary Authority of Singapore (MAS) is the central bank of Singapore.
MFS	Mobile financial services
MiCAR	Markets in Crypto-Assets Regulation See also: https://www.investopedia.com/what-is-market-in-crypto-assets-6751039
MM	Mobile Money

Term	Description
MNO	Mobile Network Operator
MVNO	Mobile Virtual Network Operator
NFT	Non-Fungible Token (NFT) See also: https://www.investopedia.com/non-fungible-tokens-nft-5115211)
RWA	Real World Asset
SEC	Securities and Exchange Commission See also: https://www.investopedia.com/terms/s/sec.asp
Telcos/ Telecoms	Companies of the telecommunications sector
UI	User Interface
USDC	USD Coin See also: https://www.investopedia.com/usd-coin-5210435
USDT	Tether See also: https://www.investopedia.com/terms/t/tether-usdt.asp
UX	User Experience. The process design of a UI, User interactions with the UI
XML	Xtensible Markup Language
ZAG	Zahlungsdiensteaufsichtsgesetz See more: https://www2.deloitte.com/dl/en/pages/legal/articles/micar-e-geld-token-crypto.html

2.6 References

Ref	Doc Number	Title
[1]	N/A	Stablecoins: Definition, How They Work, and Types https://www.investopedia.com/terms/s/stablecoin.asp
[2]	N/A	Save Money, Transact Faster: Stablecoins as an Alternative to Traditional Banking https://www.nasdaq.com/articles/save-money-transact-faster%3A-stablecoins-as-an-alternative-to-traditional-banking-2021-09
[3]	N/A	Mobile payments and telco financial services – Top 5 examples https://stlpartners.com/articles/consumer/mobile-payments-telco-financial-services/
[4]	N/A	Telco Tokenization and Stablecoin Development an Industry Opportunity https://ieeexplore.ieee.org/document/10087064
[5]	N/A	Bank for International Settlements' Committee on Payments and Market Infrastructures: Considerations for the use of stablecoin arrangements in cross-border payments https://www.bis.org/cpmi/publ/d220.pdf

Ref	Doc Number	Title
[6]	N/A	EBA provides new rules for stablecoins https://www.ashurst.com/en/insights/eba-provides-new-rules-for-stablecoins/
[7]	N/A	Stablecoins: A Deep Dive into Valuation and Depegging https://www.spglobal.com/en/research-insights/featured/special-editorial/stablecoins-a-deep-dive-into-valuation-and-depegging
[8]	N/A	Anti-Money Laundering (AML): What It Is, Its History, and How It Works https://www.investopedia.com/terms/a/aml.asp
[9]	N/A	Combating the Financing of Terrorism (CFT) Definition https://www.investopedia.com/terms/c/combating-financing-terrorism-cft.asp
[10]	N/A	The Energy Consumption of Proof-of-Stake Systems: Replication and Expansion Juan Ignacio Ibañez UCL Centre for Blockchain Technologies; The DLT Science Foundation Francisco Rua University College London - Centre for Blockchain Technologies https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4324137
[11]	N/A	Chainlink 2.0: Next Steps in the Evolution of Decentralized Oracle Networks https://research.chain.link/whitepaper-v2.pdf
[12]	N/A	SocialConnect https://github.com/celo-org/SocialConnect
[13]	N/A	NIST Stablecoin Report Highlights Security and Stability Concerns https://www.jdsupra.com/legalnews/nist-stablecoin-report-highlights-3575983/
[14]	N/A	Digital Assets - Worldwide https://www.statista.com/outlook/fmo/digital-assets/worldwide
[15]	N/A	Whitepaper of the RDDL Foundation https://static1.squarespace.com/static/6415d117eeef9450d9d98983/t/64184e907eadfe039cbce27a/1679314578865/The+RDDL+Network+-+Vision+for+a+Physical+Trust+Layer+-+v1.3.pdf

Ref	Doc Number	Title
[16]	N/A	Vodafone looks to integrate crypto wallets with SIM cards https://cointelegraph.com/news/vodafone-blockchain-integrate-crypto-wallets-sim-cards
[17]	N/A	Stablecoins versus tokenised deposits: implications for the singleness of money https://www.bis.org/publ/bisbull73.pdf
[18]	N/A	Does Crypto Pass the Howey Test https://www.investopedia.com/does-crypto-pass-the-howey-test-8385183
[19]	N/A	COVID-19 Boosted the Adoption of Digital Financial Services https://www.worldbank.org/en/news/feature/2022/07/21/covid-19-boosted-the-adoption-of-digital-financial-services
[20]	N/A	SEC's "Framework for 'Investment Contract' Analysis of Digital Assets
[21]	N/A	FCA's "Policy Statement on Stablecoins" (PS21/22)
[22]	N/A	SEC's "Statement on Digital Asset Securities Issuance and Trading
[23]	N/A	European crypto-assets regulation (MiCAR) https://eur-lex.europa.eu/EN/legal-content/summary/european-crypto-assets-regulation-mica.html#keyterm_E0001
[24]	N/A	Carbon Markets, Tokenization and the Enterprise Data Challenge https://media.meeco.me/public-assets/white_papers/Meeco_Carbon_Market_Paper-COP27-2022-11.pdf

3 Types and roles of stablecoins

Stablecoins, as a subset of digital assets, potentially offer their users relative price stability, and can be defined as digital assets designed to have a relatively stable price. Price stability can be relative to any reference asset or to a basket of currencies or assets. Stablecoins can be differentiated by

- the underlying reference asset
- the transfer mechanism
- the issuer
- stability mechanism

3.1 Categorization based on reference asset

Stablecoins can be categorized based on the underlying benchmark against which their value is stabilized. Whether linked to fiat currencies, indices, or a composite basket of goods or currencies, each reference asset type contributes to the unique characteristics of the stablecoin.

3.2 Transfer mechanism variations

Another critical aspect of stablecoins lies in the transfer mechanism, with reliance on open-source or closed-source technologies. These choices profoundly influence the decentralization, accessibility, and transparency of stablecoins, allowing for tailored solutions to meet specific needs.

3.3 Categorization based on issuer

The type of issuer plays a pivotal role, as stablecoins can potentially be issued by decentralized protocols, central banks, or private entities. Governance structures also vary, with control residing with the issuer, users, or distributed governance rights. These distinctions contribute to the overall resilience and adaptability of stablecoins in different economic contexts.

3.4 Stability mechanism classification

The stability mechanism further divides stablecoins into

- on-chain collateralized
- off-chain collateralized
- seigniorage share/algorithmic
- hybrid mechanisms.

On-chain collateralization involves securing the stablecoin value through assets on the blockchain, while off-chain collateralization relies on external assets. Seigniorage share and algorithmic mechanisms potentially introduce innovative ways to maintain stability, with algorithms adjusting the coin supply based on market conditions. Hybrid mechanisms blend elements of multiple stability mechanisms, potentially providing a balanced approach to mitigate risks and enhance overall stability.

Off-chain collateralized stablecoins are typically collateralized by credit instruments. These tokens rely on a trusted centralized third party to hold the collateral, and regulation and regular audits are necessary to build and maintain that trust. By amount in circulation the largest examples in this category are USD Coin (USDC) and Tether (USDT). These assets are governed by a central entity, and the major price risk of the token is mostly determined by the credit and duration risk of the underlying credit instruments and the counterparty risk of the institutions holding the collateral.

In contrast, on-chain collateralized stablecoins are often more transparent, as their governance and collateral can be based on open-source smart-contracts which potentially can openly be audited. The liquidation process occurs entirely on-chain, resulting in faster redemption of the stablecoin for the underlying collateral. As the collateral of on-chain

collateralized stablecoin coins typically consists of other crypto-assets the volatility and liquidity of the collateral are major drivers of price risk of these instruments.

Seigniorage share coins typically introduce a second asset, the seigniorage asset, that is responsible for taking up the volatility that comes with varying levels of demand for a stablecoin. Seigniorage-style stablecoins algorithmically expand or contract the supply of the stable token to match demand, shifting volatility risk from the coin holders to the complementary asset holders, depending on the activity of the market.

Finally, a hybrid mechanism typically relies on elements of the previously mentioned designs, e.g. combining on-chain collateral with a mechanism that expands and contracts the amount of stablecoin in circulation, depending on varying levels of demand.

4 Jurisdictional legal and regulatory ramifications of using a stablecoin

Regulatory frameworks and technologies are continually evolving. This applies to a global stablecoin arrangement if it covers several jurisdictions. It is crucial to continuously review the developments in all affected jurisdictions and to be prepared to be able to continuously adapt to the stablecoin ecosystem if necessary.

Building a compliant stablecoin ecosystem for cross-border global wholesale settlement involves a combination of technological, regulatory, and operational considerations. It is important to note, that regarding the regulatory aspects a huge difference between the wholesale and retail market exist. The requirements for a stablecoin arrangement which is used in the retail market are much higher and stronger than for a wholesale use case.

The legal and regulatory frameworks can vary significantly depending on the jurisdiction. Key areas that require evaluation include:

- Transaction regulations
- Asset management
- Tax compliance
- Security Laws
- Sanctions
- AML/CFT

Each country has its own laws regarding these international transactions. These laws can include aspects such as taxes withheld at the source and other regulations. Additionally, some governments may restrict business dealings and the export of certain goods to countries on their sanctions list. The appropriate regulatory body for each involved jurisdiction in the ecosystem (for example: Financial Conduct Authority (FCA) in United Kingdom, Securities and Exchange Commission (SEC) in the US, Commodity Futures Trading Commission (CFTC) etc.) needs to be identified before launching or utilizing stablecoins. In addition, international initiatives and organizations like the G20 cross-border payments programme (BIS (2020)), the “Bank for International Settlements’ Committee on

Payments and Market Infrastructures" (CPMI) and "International Organization of Securities Commissions" (IOSCO)'s July 2022 final stablecoin guidance, which confirms to the application of the Principles for Financial Market Infrastructures (PFMI) [5] for systemically important stablecoin agreements, should be included in the assessment.

A mapping of jurisdictions to ease of doing digital assets business from transparency and flexibility needs to be performed. To ensure a fair regulation across new and traditional financial systems, stablecoin providers will be subject to the same regulatory standards as traditional financial institutions with comparable risk profiles. Therefore, it should be assumed, that the principle of "same business, same risk or risk profile, same regulatory outcome" will be applied in international and domestic regulatory frameworks [5].

Within a stablecoin arrangement different participants may exist. On the one hand there may be founders who create and manage the consortium and act as stablecoin issuers. They may own and operate the network. On the other hand, there are potential partners who act as consumers. These are businesses in different jurisdictions that could use the stablecoin. Expanding the stablecoin arrangement to the retail market introduces retail consumers as new participants.
It is crucial to evaluate requirements of the partners and consumers as well as regulatory requirements to assess commercial viability and ensure compliance.

4.1 Regulatory and compliance framework

Integrating stablecoins into the telecommunications sector presents significant challenges. Regulatory uncertainty is currently an issue, there is lack of consistent regulation, supervision and oversight across jurisdictions [5].

The significance and need of clear regulations are seen in various regions like the European Union, United States, UK, Singapore, to name a few. Regulators such as the SEC and FCA see a need to impose his does also need to recognise that the need for appropriate financial crime standards are also in industry interests financial and prudential standards on stablecoins such as Reserve Management and Transparency, Anti-Money Laundering (AML) and Know Your Customer (KYC) Compliance, Consumer Protection and Redemptions, Operational Resilience and Cybersecurity [9, 20, 21, 22].

Regarding Europe, the EU should seek to harmonise regulatory frameworks relevant to stablecoins to enable scaled implementations across the Union without operators having to abide by a multitude of potentially differing national provisions.

From the perspective of international institutions like Bank for International Settlements' Committee on Payments and Market Infrastructures (CPMI) international standards, recommendations and guidance exist [5].

However, cross-border payments need to be reinforced by regulatory frameworks which are consistent across jurisdictions and are in line with international policies and this consistency is currently not existent.

Telecom operators and telecom service providers could use their standing to approach the regulators and explain the benefits they perceive so that the regulators have a more balanced view of the needs of the industry. This does also need to recognize that the need for appropriate financial crime standards are also in industry interests.

The regulatory framework for stablecoins seeks to elevate them to mainstream acceptance as a digital means of exchange and as a conduit between fiat and digital asset ecosystems. To facilitate this objective, several factors must be considered to establish a stable and compliant ecosystem.

4.1.1 Organisational structure of the stablecoin arrangement

A stablecoin arrangement consists of different entities and building blocks (see chapter 8.4.2 The Building blocks). Although a cross-border capability is one of the key features of a stablecoin arrangement, the system's key components should not be geographically dispersed. There are trivial arguments like time differences. The more significant fact is, that for the different jurisdictions different standards and policies exist, e.g., regarding KYC/AML implementations and on and off-ramp systems. Furthermore, to enhance security and robustness, both the issuer's legal entity and the management of reserve assets should be located within the same jurisdiction.

4.1.2 Value stability

Value stability is crucial to gain confidence for potential partners, customers, and investors. It depends on many influencing factors from different domains:

- The overall economic environment where market volatility, liquidity stresses, financial market events, counterparty performance, and the balance of demand and supply impacts the price stability.
- The market behaviour decides on the adoption of the system.
- Governance to assure the right management of reserves and collaterals.
- Technical domain with operational stability and maturity, vulnerabilities to hacks, technological design with respect to evolvement and scalability

Finally regulatory certainty and a stable legal foundation are key success factors [7].

4.1.3 Redemption

The objective from regulatory point of view is always to ensure that holders of an asset-backed stablecoin can redeem their tokens at par value. Stablecoin issuers should enable prompt redemption and disclose their redemption policies.

4.1.4 Disclosure

The rules and policies which applies to the stablecoin arrangement should be made public. The policies must clearly state about settlement finality and the transfer of coins must be adequately documented once it has become irreversible.

Other aspects of the public disclosure should comprise the “Supply and redemption” mechanism as well as how reserve asset management is organized, especially how the portfolio of referenced assets looks like.

4.1.5 Risk requirements

Risk requirements are vital within a regulatory and compliance framework. This fact is critical as to assure stablecoin issuers that they comply within the jurisdictional laws, regulations,

and industry standards. Risk requirements are described in detail in chapter 5 of this whitepaper.

4.1.6 The view of central banks and regulators regarding a compliant Stablecoin Arrangement

A systemically important stablecoin arrangement which are used globally in cross-border payments may have impact on the financial stability and therefore requires adaptation on monetary policies [5].

Central banks objectives [5] include “(i) fostering safe, reliable, transparent and efficient payment systems; (ii) promoting monetary stability; and (iii) promoting financial stability.” These objectives need to be considered in any stablecoin arrangement.

The currency backing a stablecoin can significantly influence traditional financial stability: (1) High demand for a stablecoin pegged to a currency with strict capital controls can create challenges. (2) Additionally, a run on a stablecoin system can strain the operations of off-ramp entities, particularly those also involved in traditional financial services.

Cross-border payments have a different impact regarding Emerging markets and developing economies (EMDEs) as on Advanced economies (AEs). In countries classified as EMDEs typically there is a higher use of cash and more people do not have access to classic payment services offered by banks. In these countries a stablecoin could get a higher share of financial services and could therefore have more influence on financial stability. This is true especially when the stablecoin has a wide acceptance and is treated as systemically relevant. When the stablecoin is denominated in a foreign currency and is operated from a foreign jurisdiction, the acceptance in EMDEs, where the domestic currency is weak, may also be higher than in AEs. Thus, for EMDEs, there exists a higher risk of currency substitution. Regulators in EMDEs might apply different regulations than regulators in AEs where currency substitution is not seen as a risk.

4.2 Licensing and registration requirements

The licensing and registration requirements for a compliant stablecoin ecosystem depend on the jurisdiction, as there exist various regulatory frameworks for digital assets and financial services. The design of the stablecoin ecosystem requires a banking or an e-money license to operate as a financial institution.

Typically, an effective registration or licensing system facilitates the gathering of essential information and data required for thorough supervision, oversight, and monitoring of potential financial stability risks. Licensing entails meeting prudential standards, including initial capital requirements. Regulatory authorities will also prioritize safeguarding individual user privacy.

In general, a proper registration or licensing regime allows the collection of information and data necessary for adequate supervision and oversight as well as for monitoring potential financial stability risks. Licensing will include prudential requirements such as initial capital requirements. Authorities will also seek to protect individual user privacy.

As a benefit for stablecoin issuers licensing and official registration will increase the confidence of all ecosystem players such as partners and end-users.

4.3 Regulatory trends and developments by region

Each telecom operator or service provider might want to review country rules and regulations including policies regarding:

- Fraud control
- Governance
- Monitoring and reporting
- Sanctions
- Accounting treatment
- Infrastructure
- Conversion costs, timing, and available market/agents
- AML/CFT

Accepting stricter regulations would provide more certainty to the CEOs and top management decision makers. Also, it increases the trust of the customers if the stablecoin arrangement is fully supported by the authorities' guidelines. Authorities and regulators will also request to be fully compliant with policies.

The disadvantage of having stricter rules is that the space for innovation may narrow and competitors in a world-wide contest might gain market shares due to innovative new features. Moreover, required investment into the compliance may be higher.

Another aspect to consider is the fact that most of the telecoms are multi-national companies engaged in many different jurisdictions. Hence, to establish a stablecoin model for the industry, every participating telecom company would need to guarantee that the stablecoin meets the approval of its respective domestic telecommunications regulator. Since numerous telecoms operate across various markets, a thorough examination of the regulatory frameworks in each relevant jurisdiction would be necessary. Quite apart from the views of the telecom's regulators, the central banks and financial regulators in such jurisdictions will also require local oversight and regulation, especially when the stablecoin arrangement is considered as systemically relevant. As an example, would EU-based telecoms be permitted to transact with a Singapore-regulated stablecoin, or vice versa? The consortium could also consider partnering with a bank (or consortium of banks) that has existing stablecoin experience to help in the regulatory approval process.

One particular concern for regulators might be that a stablecoin arrangement is intended for retail customers who would operate their own mobile wallets and purchase and use the stablecoin. There might be less regulatory concern if consortium members would intend to use the stablecoin only for the purposes of transacting amongst themselves on a wholesale basis. Therefore, one aspect on the decision about the appropriate jurisdiction is the line of business the stablecoin arrangement is built for.

A potential strategy to help address risk in a consortium's plans would be to (at least initially) utilize the stablecoin only at a wholesale level whilst consumer functionality might be added later. From a regulatory perspective, it may be easier to launch and implement solely at a wholesale level, for example to settle roaming payments. Also, a suggestion may be to roll out localized compliant variants which are meant for country specific transactions and where regulators of two regions allow cross country transactions under a common regulatory regime these potentially could be launched as well.

5 Accounting and reporting requirements

Accounting standards enable various companies and institutions to function within a unified financial system. The right accounting has several key benefits for the stablecoin arrangement. Among other things, a proper accounting provides

- Transparency, means a clear and transparent financial information
- Compliance, means to assure that that companies comply with legal and regulatory requirements
- Global Integration: International standards like IFRS facilitate global business operations by providing a common financial language, which is particularly important for multinational companies.

All the points above increase investor confidence since they help providing a true and fair view of a company's financial health.

Accounting and reporting requirements apply as well to the issuer of stablecoins as well as to businesses, who act as users of the stablecoin ecosystem, who then hold stablecoins. Telecoms that are not members of the issuing entity, as well as those that are, can use the stablecoins arrangement. Members of the issuing entity may also act as users in addition to their role as issuers.

As already stated in chapter 4.3 of this paper: "… most of the telecoms are multi-national companies engaged in many different jurisdictions. Hence, to establish a stablecoin model for the industry, every telecom company would need to guarantee that the stablecoin meets the approval of its respective domestic telecommunications regulator". This statement also applies to the use of accounting standards.

5.1 Accounting standards

Telecoms operate in multiple jurisdictions and must comply with both national and international accounting standards. For instance, in Germany, companies follow the national Handelsgesetzbuch (HGB) and International Financial Reporting Standards (IFRS) for their accounting practices. Various accounting standards are applicable to institutions both within the U.S. and globally, such as:

- U.S. Generally Accepted Accounting Principles (GAAP): GAAP, is the main set of accounting standards used by both public and private organizations in the U.S. Compliance with GAAP is mandatory for all publicly traded companies.

- International Financial Reporting Standards (IFRS): These standards are used internationally and are issued by the International Accounting Standards Board (IASB).
- National accounting standards

5.2 Classification

Telecoms should determine the appropriate accounting treatment for the stablecoin. This means to clarify to which kind of asset a stablecoin is based on their business context and the nature of their digital asset operations and strategies, and then apply the appropriate accounting standards.

- Financial instrument (including cash or cash equivalents)
- Intangible asset
- Another category depending on its characteristics, e.g. as “Inventory”

This decision establishes precise accounting guidelines regarding the allocation of assets to the balance sheet, as well as serving as the foundation for determining relevant tax implications. While a detailed explanation of accounting is beyond the scope of this paper, the following classification rules are presented to give an impression of its complexity:

Classification as “Financial instruments”

Stablecoins may qualify as a financial instrument, when stablecoins are redeemable on demand. The initial measurement calculates the fair value of the stablecoin. For subsequent measurement telecoms must implement consistent measures to calculate the value of the stablecoin (to measure changes in the fair value). This includes the definition of selected exchanges as reference sources. The appropriate value determination can be achieved by applying periodic assessments of the stablecoin's market value, particularly by requesting the selected exchanges. Transaction costs decrease the revenue, and they may need to be capitalized or expensed based on the nature of the transaction.

Since the proposed stablecoin design in this paper includes redemption functions this kind of stablecoin may be treated as financial asset.

Classification as “Intangible assets”

As stablecoins lack physical form but offer future economic benefits, they may qualify as intangible assets. Under IFRS an intangible asset is defined as an identifiable, non-monetary asset that lacks physical substance.

Classification as Inventory

Companies, whose primary business model focusses on buying and selling stablecoin, may need to capture stablecoins as inventory on their balance sheet. Especially this may apply to those companies who are member of the issuing entity.

The correct classification also depends on whether a company is part of the issuing entity or if it is a user of the stablecoin, holding it as a means of exchange. In the former case the

stablecoin should be treated as liability as the issuer has an obligation to redeem the stablecoins for their underlying assets or fiat currency. For users, the stablecoin is always an asset.

5.3 Stablecoin characteristics to be considered for accounting purposes

To accurately classify a stablecoin on the balance sheet, the following key questions, among others, should be addressed:

- How is the stablecoin stabilization mechanism designed?
- If there are collaterals used, which kind of collaterals are used and how are the collaterals verified?
- Is the stablecoin tradeable?
- Who is the issuing entity and what legal form the entity has? Which regulations apply?
- Is the stablecoin redeemable and if so, what are the terms and conditions?

6 Risk Management

6.1 Areas of risks

Risks to be considered as part of stablecoin implementation are presented below. Systemic and idiosyncratic risks to a stablecoin settlement project need to be defined.

6.1.1 Financial crime

The design and usage of stablecoins can expose them to various forms of financial crimes like Money Laundering (ML) [8] and Terrorist financing (TF) [9]. To address both risks, AML, and TF, the so called “Travel Rule for CASP” has been formulated by the Financial Action Task Force (FATF). To fulfil the AML/FATF requirements a real time transaction monitoring is necessary.

Another key financial crime issue is compliance with economic sanctions law in relevant jurisdictions. A central management of the stablecoin would be required to adhere to sanctions in place across major jurisdictions, including UK, EU & US and UN.

The use of a stablecoin with the right controls could however solve payments issues currently observed with non-sanctioned parties in high-risk jurisdictions

6.1.2 Data privacy and protection

In a retail environment where a stablecoin ecosystem is accessible to businesses, users should maintain control and provide consent regarding their personal data. Stablecoin issuers, service providers, and entities linked to the stablecoin system must comply with national privacy regulations to safeguard user information. Here, "national" pertains to the jurisdiction where the service is provided to end-users. In a purely wholesale settlement scenario, information protection extends to enterprise data, too.

Data privacy in the context of stablecoin usage has two key vulnerabilities:

- User consent and control
- Regulatory and compliance challenges

Regarding user consent and control, the user interface must support a clear understanding for the collection and use of user's personal data, and, especially given the complex nature of stablecoin transactions the UI and UX should provide a certain layer of abstraction. By using abstraction, e.g., by hiding the technical complexity and translating technical and process complexity into a higher-level user language, the usability is increased, and the user gets more of an understanding about his or her actions and outcome.

Privacy regulations such as the General Data Protection Regulation (GDPR) in Europe have a direct impact on how user information shall be collected, stored, and processed. Regulations such as the GDPR can only be implemented using strict privacy and security measures.

6.1.3 Liquidity

Liquidity stresses, caused by high market volatility, may impact demand, and distort the stablecoin's price from its peg. The risk of losing the peg depends on the stablecoin's stabilization mechanism.

Whatever stabilization mechanism is implemented, if it breaks down, and the market loses confidence in its ability to maintain the peg there is a high risk of a "bank run". In this context, a run could also be instigated by a sudden loss of confidence in the stablecoin, potentially leading to a self-fulfilling and self-reinforcing cycle. Such a run might occur due to speculation or deliberate attacks by short sellers on the stablecoin protocol.

When "Automated Market Makers" (AMM) are used as an exchange to convert tokens to prices it is essential how the AMM implements its core exchange function. AMM provides a fully automated and decentralized approach for exchanging asset tokens and calculating prices based on demand and supply. An AMM automates this by allowing participants to place orders with the AMM, which then algorithmically provides a price. This algorithm is the heart of the exchange function. Next to the exchange function it is a responsibility of the AMM to maintain enough quantities of tokens in the liquidity pool.

Also, every AMM operates with competitors in the market and the AMM relies on arbitrage or oracles to align prices with the broader market.

It is essential for an issuer of a stablecoin to assess the above mentioned types of an AMM design and to review the historical results – especially in times of stress in the market - regarding price stability and liquidity of different AMMs before an AMM is selected.

6.1.4 Custody

Digital asset custody describes various measures to store and protect crypto assets on behalf of their owners. Technically, custodians do not maintain the assets but the cryptographic keys which grant access to the assets.

Regarding custody management mainly two different approaches exist: (i) use of a centralized entity or (ii) fully decentralized.

If stablecoins are issued and managed by centralized entities, the custodianship of funds, the security of the underlying reserves and finally, trust are dependent on this one entity. These custodians are called “Institutional Custody Services”. One option is that financial institutions manage investors’ digital assets not themselves (direct custody) but use a sub-custodian. This approach has the advantage that the core custodian functions (storing, protecting, transferring assets) are processed by a specialized organization.

Centralized custody presents a risk of undermining the integrity of the central entity's system, potentially resulting in theft or loss of assets if the entity has insufficient security measures in place. Conversely, custody services for digital assets provided by centralized entities such as banks, exchanges, and other financial service providers are important for maintaining investor confidence. Mitigating the risk associated with a centralized custodian entails conducting thorough assessments of multiple providers and seeking guidance from partners with prior experience in establishing a crypto asset management system.

Fully decentralized custody service is realized by decentralized finance platforms, and they potentially offer custody solutions through smart contracts. Users have control of their private keys. However, also by using a decentralized approach there is a dependency, namely the dependency to the smart contract implementation, its maturity and security.

As a third potential option a stablecoin arrangement could decide to use self-custody solutions. The potential advantage is that all functions are under control and fully transparent.

6.1.5 Collateral

The members of the issuing entity need to provide the funds to setup the collaterals when using a stablecoin which is backed by real world assets.

If the collateral is built using assets other than cash reserves, such as real-world assets like short-term debt obligations (T-bonds), they are subject to market trends and volatility. In the worst-case scenario, the collateral's asset value can decline rapidly, as was observed with bonds in the spring of 2023 following a rapid rise in interest rates. Increased bond yields usually result in lower bond prices.

6.1.6 Governance

In the context of a stablecoin arrangement the term “Governance” typically describes the mechanisms and processes by which decisions are made and the stablecoin system is managed. One of the core aspects of governance is the management of reserves and collaterals for stablecoins when they are backed by real world assets. The governance directly influences the stability of the stablecoin's value, and mismanagement can lead to a decoupling from its peg.

Setting up governance between different members, all coming from different jurisdictions with different technical and business processes make it challenging.

The decision whether telecoms should form their own consortium or not, is a fundamental decision.

6.1.7 Transactional finality

By employing DLT, business functions and associated payment functions are integrated within a single transactional context. This seamless integration presents a significant advantage of DLT over the traditional approach, where separate technology stacks are required to implement business logic and payments. Such transactions benefit from the embedding of payment functions, potentially reducing risks, especially those related to payment and settlement.

Transactional or technical finality refers to the irreversible confirmation of a transaction on a DLT and it ensures that parties involved can trust the immutability of the transaction history. Various blockchain networks utilize distinct consensus algorithms, each employing a unique approach to validate transactions and guarantee finality. As this white paper deliberately does not contain any technical decisions, it is important for the solution outline to formulate how transaction finality will be achieved.

Technical transactional finality is the foundation of a decentralized payment system since it enables finality of payment and contractual finality.

In finance, "finality of payment" denotes the instant when funds, transferred from one account to another, formally become the legal property and ownership of the receiving party. Transactions and the transfer of ownership must be irrevocable and final – otherwise balance sheet items on the sender and receiver organisation side are not definitive.

Ultimately, the legal system and contractual agreements must establish the link between the claim on or ownership of the underlying asset and the record of the digital token. This is the level of contractual arrangements and contractual finality in this context means, that the underlying transaction between parties is also contractually settled. This implies that like a conventional financial system, a decentralized financial system requires robust support from an effective legal and judicial system, along with institutions capable of enforcing contractual agreements.

The term “contractual finality” as used in this section should not be confused with “smart contract finality”. Smart contract finality ensures that the rules as programmed in the smart contract are enforced and after execution finally committed, and parties can rely on the outcome without the risk of modification. But this kind of contractually finality is still on the technical level.

6.1.8 Other risks

Other risks in the context of a stablecoin arrangement include:

- Licensing regime uncertainties (for instance in US whether SEC or CFTC to regulate)
- Cyber/IT resilience and protection risk
- Smart contract audit and accuracy risk
- Monetary policies risk
- Financial stability (and thus the reaction and measures of regulators and authorities)

6.2 Tools and processes to mitigate risks

The following operational, financial and compliance tools are needed at a minimum to maintain financial integrity and safety of the stablecoin platform designed and implemented for the setup and maintenance of a stablecoin based payment system.

6.2.1 KYB / KYC

Dependent on the chosen type of DLT, the onboarding of new network members is organized in different ways. A permissioned network setup as an initial setup for the telecom industry is ideal for providing a solution for wholesale payments. Based on this assumption, in a permissioned consortium network, when participants know each other and there is a certain level of trust between them, then the onboarding process can be realized by using node-permissioning and account-permissioning functions.

“Know Your Customer” (KYC) functions are required when the telecoms’ DLT solution is extended by retail use cases. KYC is a legal requirement to verify their users' identities.

KYC should consist at least of the following functions:

- Digital ID analysis and verification
- ID proofing, document and biometric authentication (including liveness tests)
- Public/Social/private data sources mining, where the public and social part applies only to the onboarding of private customers
- Trust scores
- Fraud mitigation and AI based fraud analysis
- AML compliance

6.2.2 Real time Transaction Monitoring and Sanctions screening

All transactions and login attempts, and other actions performed on the system need to be monitored in real time to comply with regulatory requirements and to offer transparent business processes.

Sanctions screening serves as a mechanism to identify and deter financial crimes, thereby ensuring adherence to AML/KYC regulations. This screening process enables telecoms to conduct checks on their records against sanction lists, to avoid engaging in business with entities listed on politically exposed persons (PEPs) or sanction lists.

Realtime monitoring and sanctions screening enable following features:

- Investigate, trace and track suspicious transactions
- Connecting DLT transaction to real world entities
- AML/CFT compliance

- Address screening including sanction and high-risk list monitoring
- Generate high quality alerts
- Enhanced due diligence for suspicious activity or selected jurisdictions
- Travel Rule pre-transaction decision making
- Automated and continuous address, wallet and transaction screening in real time
- Support across protocols and currencies

6.2.3 Exchange (for Trade/Swap) and Market

To swap a local stablecoin to international stablecoin an exchange is needed. An exchange is also needed for the conversion of fiat currencies to the stablecoin. The decision to be made for setup of the stablecoin arrangement is if a central exchange or decentralized Automated Market Makers (AMMs) shall be used.

The main requirements regarding an exchange are to provide an appropriate liquidity pools management concerning the stablecoin pair as well as the support of oracles to consume market data and to adjust price findings from other exchanges.

Price volatility risks, counterparty risks, liquidity risks and security risks need to be addressed when dealing with an exchange. In addition, the exchange should support instant settlement to prevent transfer risks as delays could result in losses due to market fluctuations.

6.2.4 Embedded finance

The stablecoin payment platform needs the following components and functions to integrate the stablecoins into the traditional financial system:

- On/Off Ramp providers (to support deposits and withdrawals)
- Authentication and connectivity pipes to bank accounts (if used as source of funding)
- Card/Payment gateways
- Cross-border payment service provider (with appropriate license)
- Connectivity to carrier mobile wallets if needed (either direct or through B2B aggregators)

All the above-mentioned functions and components are part of the building blocks of a stablecoin arrangement and in general, for all these functions and components the following risks need to be managed:

- Security risks
- Regulatory and compliance risks
- System stability (implementation and runtime) risks

Additionally, there are specific risks that require attention:

As the stablecoin arrangement will facilitate cross-border payments, especially for the on- and -off ramp infrastructure there is the risk of inconsistent regulation, supervision and oversight across jurisdictions. All the above-mentioned functions must be integrated in every jurisdiction, and it should be in a harmonized consistent way. But the situations is: Different regulations exist, different existing payment infrastructure, different market integrity conditions, etc.. The differences between emerging markets and advanced markets make it even more challenging to implement a consistent stablecoin arrangement for all involved jurisdictions.

6.3 Insurance and support policies

As much as blockchain and decentralised networks reduce the single point of failure risk, there exist several risks present along the entire ecosystem required to deploy stablecoin solutions for wholesale settlement. To safeguard both individuals and institutions, it's advisable to assess insurance coverage for institutional funds and protection against cybersecurity threats as an added layer to mitigate the impact of specific risks.

Telecoms should therefore seek insurance partnerships and explore partnerships with insurance providers to cover potential risks, such as smart contract exploits, operational failures, or regulatory changes might need to be considered.

6.4 AI-Enhanced Risk Management

In the context of a stablecoin based payment system artificial intelligence (AI) can leverage the analysis of historical data, market indicators, and real-time information.

AI encompasses several tools and methodologies, particularly focusing on recognizing and interpreting patterns to identify market volatility, liquidity trends, and signs of fraudulent activities or manipulation attempts. AI achieves this through the utilization of techniques such as "Machine Learning (ML)," "Natural Language Processing (NLP)," and historical analysis of Distributed Ledger Technology (DLT) data. Analysing historical data enables the creation of predictive models that calculate the likelihood of a stablecoin deviating from its peg. Important to note is that any AI technology used to enable stablecoin capability must comply with the telecoms responsible AI program which may embed “Security and Trust by Design” as well as adhere to appropriate regulation and legislation such as the EU AI Act (for telecoms residing in the EU).

In summary, leveraging AI technology serves to mitigate risks while simultaneously enhancing the confidence and trust of partners and investors.

7 Stablecoin design

In this chapter the term “system” refers to the to be implemented telecom stablecoin arrangement implementation.

7.1 Vision

Given the geographic dispersion, capital, and local market knowledge telecom enterprises collectively possess and the fragmented state and lack of global standard for USD and Non-

USD stablecoins, a consortium of telecom companies could consider capturing the global market for stablecoins and foreign exchange on public DLTs.

7.1.1 Stablecoins in every jurisdiction

Such an approach may involve, telecoms launch stablecoins in their local jurisdictions, backed one-for-one by short term treasuries and bank deposits held in trust, earning a risk-free rate in their currency and enabling their users to store fully backed, tokenized currencies on public ledgers and transfer them independent of third parties, at efficient costs, at any time, without reliance on costly intermediaries, as seamlessly as a text message.

7.1.2 Global standard for stablecoins

The industry could potentially launch a global stablecoin API that enables companies to integrate every stablecoin on and off ramp from their partners into their mobile applications in one integration. This may enable the industry to innovate the existing stablecoin marketplace, which is highly fragmented and requires partnering with new service providers, integrating banking and technological systems for each stablecoin in every jurisdiction.

A new global API for payments enhances existing stablecoin marketplace by reducing fragmentation. Particularly,

1. Stablecoin issuers are highly localized and thus fragmented, requiring the integration of new technological, banking, compliance systems from third parties into applications in every jurisdiction to use them.

2. By creating a global API that can be used by all the member's and consumers of the stablecoin arrangement. On- and off-ramp facilities for their stablecoins are built into one application, this removes the need to integrate each new issuer individually.

The advantages of building a solution based on a global standard and the benefits of telecoms are:

- Source of income: Telecoms may earn yield from treasuries in their local currency by backing stablecoins with treasuries, earning a risk-free rate based on their customer's demand to self-custody, transfer, exchange their stablecoin on public blockchains. Additionally, telecoms may earn on- and off-ramp fees, exchange fees from providing liquidity (from trades), by charging transaction fees in their apps, and as market makers by purchasing stablecoins when they go below their peg and redeeming them for the underlying profit at no redemption costs.

- Lowest risk: Buying treasuries and holding funds in trust to back each stablecoin 1-for-1 may mitigate risks of bank runs.

- Global ubiquity: Creating a global standard for stablecoin implementation may enable the tokenization of the global FX and money transfer markets on public DLT/ blockchains, potentially removing the need for expensive intermediaries and positioning with a potential opportunity.

- "Infrastructural optionality" for corporate treasurers and asset managers

A global standard solution comes also with challenges like a high coordination effort to enable collaboration between the different entities in the ecosystem like issuers, banks, and regulators. It requires smart contract development, maintenance and operation knowledge and systems.

A global standard potentially tackles also the current lack of Non-USD denominated digital assets and on-chain FX markets. As evidence of this fragmentation, 60% of the global currency reserves are USD, but 99% of current on-chain digital money is USD denominated. This presents first mover advantage opportunities.

In addition, there is a lack of connected / embedded on- and off-ramps and UX. Even if there was strong liquidity for non-USD digital money, to bring real value to consumers, “real world functionality” remains a missing link: Even if you can transact instantly for fractions of the cost into a digital representation of your currency, if you can’t pay rent or buy a cup of coffee with it, it’s not that useful.

7.1.3 Global standard for on-chain foreign exchange (FX)

By tokenizing currencies globally, this potentially enables members of the issuing entity and their customers to provide stablecoin liquidity to automated, self-custodial, decentralized exchange markets on DLT / blockchains and earn yield from trades while benefiting from more available, efficient markets which may offer significant risk reduction in FX execution, settlement, and treasury management.

7.1.4 Integration into the Mobile Financial Systems (MFS)

Open loop stablecoins are backed by local currency bank deposits and equivalents, they include mostly short-term treasuries held in segregated, trust-based accounts. Stablecoins in the network may be connected to local Mobile Financial Systems (MFS) payment rails, which are potentially accessible to participants via a single integration for on- and off-ramping their mobile application customers into and out of local stablecoins in other jurisdictions using local payment rails.

7.1.5 Collateral and Fund Storage

Telecoms back stablecoins in their local jurisdiction with short term treasuries and bank deposits that are held in segregated accounts with 100% collateral backing the tokenized representation. At any time, funds may be redeemed one-for-one with the underlying. Another potential option is to introduce an eSDR backed stablecoin, since SDR is already familiar with operators today [4].

7.1.6 Interoperability and Cross-Chain Capabilities

Interoperability is one key feature required to build a network of decentralized networks, where each decentralized network reflects one business case and where the need is to cooperate. Interoperability potentially becomes relevant when incorporating additional use cases or retail applications beyond the initial (wholesale) use case. A potential advantage of a network of decentralized networks is, that each isolated decentralized network can realize the rules and entities of one business domain. This approach may provide a highly cohesive system which is easier to develop, test and maintain from that one domain perspective. Whenever it makes sense from the business point of view the isolated decentralized networks may cooperate. However, the overall complexity and vulnerability of the integrated

system may increase as more integration points (either using relays, bridges) also must be developed, tested, and maintained. The integration point itself is potentially an additional surface for attacks.

From the business architecture point of view the exchanged data need compatible semantics where the entity from one DLT retain its identity and characteristics.

7.2 Use Cases

7.2.1 Fiat-to-stablecoin conversion

On-ramps may be provided to support the deposit from an Automated Clearing House (ACH), bank transfer systems, card rail source or mobile wallets balance. ACH or real time payments (e.g.: SEPA) may be preferred due to their low fees model. An on-ramp rail from a fiat balance outside the wallet to a stablecoin held in the wallet is considered as a “deposit” to a “self-custodied” stablecoin. The stablecoin shall only be released (either through the burn process or from its own wallet) when the fiat money is settled and reaches its bank account. It should also be decided if a user is able to move their stablecoin from a different blockchain network into a wallet provided by the network of the system.

7.2.2 Stablecoin-to-fiat conversion

Off-ramps are provided to support the withdrawal into bank accounts or other fiat payment systems like ACH or card rail source. In the withdrawal process, the system must support a conversion process into the local currency as preferred by the user. The withdrawal or off-ramp must support transfer of fiat currency into user’s bank account or preferred mode of receiving the payment (e.g.: Debit card, Mobile wallet etc). An aggregator may be needed to connect to multiple operator mobile wallets if a one-to-one connection is resource intensive.

7.2.3 Stablecoins Swap / Trade - AMM liquidity pools/Centralised exchanges

The system may be used as an interface to interact with approved decentralized financial platforms, namely Automated Market Makers (AMMs). Due to challenges posed by centralised exchanges (including trust and custody), AMMs may be proposed for the system. The application may interface with approved AMM liquidity pools facilitating swaps between various stablecoins (e.g.: e-USD to e-SDR and vice versa). AMMs such as DFX may already provide trade functionalities between various stablecoins. The AMMs need to be able to offer attractive prices with minimal scope for arbitrage. Slippage needs to be minimized through higher liquidity in the platform. Hence sufficient incentives need to be offered to liquidity providers to cover for their impermanent loss. More than one AMM could be considered to provide better pricing and liquidity. In general, liquidity pools need to provide better pricing for trade (post fees deduction) compared to traditional forex brokers and banks offering such services. All stablecoins or digital assets listed on the AMM need to pass the “Howey test” [18].

7.2.4 Stablecoin transfer from one digital wallet to another

Stablecoins may be transferred in or out of the system’s wallet with each other and optionally from other compatible protocols (Ethereum Mainnet or Polygon sidechain etc). Where supported, wallet users of the system (such as MNOs participating in this project) could send

and receive stablecoin assets to and from other wallet users, via their digital asset balances. A user potentially needs only to hold any stablecoin in their wallet, then may have the option to ideally convert it into the recipient's local stablecoin currency in case the wallet supports multiple stablecoins. The swapping and conversion between stablecoins within the ecosystem may be done seamlessly potentially without the user ever needing to know and act on execution. In the case of a single stablecoin platform this may be rather more straightforward and would be just a transfer from one wallet to another on the blockchain. Eventually, the recipient users may be able to off-ramp stablecoin to a local method (e.g.: local currency) that is compliant and available. A recipient should also be able to hold it as stablecoins in their wallet if that is the preferred method. In general, holding and doing a bulk conversion (in a wholesale context) and transfer to their bank account may be cheaper.

Special design considerations are to be made if the recipient doesn't have any DLT/ blockchain enabled system app installed on their mobile device and wish to authorize the incoming transfer directly into their bank account. In order to accept the incoming stablecoin remittance, the user may still need to authenticate and authorize the transfer through an alternative portal (e.g., Web View) once they receive the SMS notifying them of the incoming transfer.

7.2.5 Card Payment (Virtual card) from Digital Asset

The use of stablecoin balance as funding source to pay for merchant goods and a payment card (Virtual Visa/Master) may allow the user to leverage an existing traditional payment system to clear a fiat payment to a merchant from their stablecoin balances.

7.3 Building a compliant ecosystem

It becomes essential to understand the regulations and various aspects of stablecoins to build an ecosystem which is compliant and keeps the industry stable as well as prevent any potential scams and frauds. Stablecoins regulatory framework aims to bring stablecoins in mainstream as a digital medium of exchange, and to serve as a bridge between the fiat and digital asset ecosystems. To facilitate the same, the following factors as depicted in the below sub chapters are to be considered for a stable and compliant ecosystem.

7.3.1 Attestation and monitoring to enable value stability

Stablecoin issuers are expected to obtain independent attestation, such as by external audit firms, that the pool assets meet the requirements on a regular basis. The attestation, including the percentage value of the pool assets in excess of the par value of outstanding stablecoins in circulation, has to be published on the issuer's website and submitted to the regulators by the end of the attestation period. Regulators also prefer issuers to appoint an external auditor to conduct an annual audit of its pool assets and submit the report in relation to its compliance with regulatory requirements.

In addition to the post-event audit function, automated verification functions can be integrated on-chain. Before new tokens are minted, a smart contract automatically verifies a reserve contract, which is synchronized and updated by oracle services with the current reserve amount. Minting is authorized only when there are adequate reserve assets available to support the new tokens.

7.3.2 Appropriate asset backing to enable value stability

Participants potentially need to define issuers are expected to hold all the pool assets used to back the stablecoin in circulation in segregated accounts, separate from its own assets which are not pool assets. The pool assets may be held with licensed banks, merchant banks, finance companies providing custodial services. This is to mitigate risk of misuse of customers stablecoins from the commingling of assets.

One of the valuing measures is to have a mark-to-market basis and be equivalent to at least 100% of the par value of the outstanding stablecoins in circulation (including those always held by the issuer).

Pool assets must be held in the form of cash, cash equivalents and may be issued by

- The reserve bank of the pegged currency; or
- Organisations that are of both a governmental and international character with an acceptable credit rating

The pool assets currency shall be the same currency as the pegged currency.

7.3.3 Authentication

The owner of private keys for the wallet need to be defined. Different models potentially available are single key (self-custody), multi signature wallet or fully centralised/custodial wallet (as provided by exchanges). To build trust and provide full transparency, a multi signature wallet (e.g., 2 out of 3 keys) could be considered where the industry will only hold one of the three owner keys. A second user key is generated by the user on the user's device and resides there in a manner secured by the smartphone device's security model. A third network key may be generated and stored in a secure manner by a trusted third party. The trusted third party can be either a globally managed key custodian or by a local partner in the jurisdiction of the user (e.g., a local IT services provider in the same jurisdiction as the MNO).

The network third key may only be used to either regenerate the user key (lost or stolen device) or in response to a lawful request from authorities in the jurisdiction of the user (e.g.: a lawful request to freeze the user's assets). The network key also ensures that, even in the event of bankruptcy or other disruptions in the business operation, users of the wallet will always have access to their funds.

7.3.4 Onboarding / eKYB/ eKYC

This section covers retail as well wholesale users.

Users need to submit documents for ID/mobile number, pin code verification and complete the eKYB/eKYC/Onboarding process. Terms and Conditions (T&Cs) must be listed in the app. An eKYB/eKYC must be performed for all potential users at the point of onboarding. T&Cs governing the contractual relationship (e.g.: disclaimers, liability, licensing etc) between the wallet of the system and the users need to be also embedded within the app at the point of sign off. Mobile number verification can provide frictionless experience (i.e. associating an identity of a wallet to MSISDN) and various fraud management tools can minimize messaging fraud. An additional layer of authentication (e.g.: 6-digit PIN) is also

necessary to conduct transactions. Optionally, biometrics (e.g.: facial scan) can also be considered as an additional authentication layer.

The documents that are part of eKYB/eKYC process are to be defined (e.g.: photo ID such as passport or license, business profile document, director info etc.) and the user should also take a photo of themselves to confirm their identity and several “liveliness” photos to prevent fraudulent applications. KYB/KYC information provided by the user can also be used to check against different databases, including government databases, to perform the true authenticity of the identity which is collected. It enables the system to fulfil the regulatory and legal obligations.

Furthermore, customer screening (e.g.: politically exposed or sanctioned individuals), transaction monitoring (suspicious activity monitoring using AML/CFT tools) are also essential operational tools to be maintained for meeting regulatory requirements across various jurisdictions.

7.3.5 Transaction monitoring

Distributed ledgers immutably store transaction history such that flows of assets are available to tools that can perform “after-the-event” analysis. Solution providers potentially offer these capabilities. Starting with a suspicious transaction, tools can track transactions that led to an event (source of funds) as well as transactions that occurred after an event (destination of funds). Not limited to a single public ledger, these tools are also able to analyse how assets are transferred from one ledger to another via bridges for a complete end to end view of the assets’ travels within and between distributed ledgers. This information may be made available to law enforcement agencies.

7.3.6 Custody

The adoption of stablecoins by digital asset markets relies heavily on integration with major commercial custody providers globally. Custody solutions have seen increased adoption, acting as core financial infrastructure for web3 applications, enterprises, and financial institutions. By ensuring support from leading custody providers, stablecoin assets and standards can be easily integrated into the applications and ecosystems already utilizing these custody solutions.

When developing new stablecoin standards, easy integration by major custody providers is critical to reduce friction for market adoption. Solutions like Fireblocks provide the security, ease of access, and revenue opportunities that institutions require to adopt new stablecoins. By prioritizing integration with key custody solutions, a newly proposed stablecoin may tap into the applications and institutional clients already relying on them.

7.3.7 Capital requirements

The capital requirements for stablecoin issuers vary across jurisdictions and they are dependent on the design of a stablecoin arrangement (stabilization mechanism, underlying asset etc.) and the regulatory frameworks in place.

To provide an example and a rough impression about capital requirements a concise overview about the situation in Europe, is outlined below.

In Europe the new Markets in Crypto Assets regulation (MiCAR) is the reference for stablecoin issuers. With respect to stablecoins MiCAR distinguishes between the following two types of assets:

- **e-money tokens** (crypto-assets that stabilise their value in relation to a single official currency);
- **asset-referenced tokens** (crypto-assets that stabilise their value in relation to other assets or a basket of assets);

The capital requirements mentioned in MiCAR only apply to asset-reference tokens: MiCAR states that it is required to "maintain at all times a reserve of assets covering the liabilities towards the holders of the tokens, and have own funds at least equal to the highest of the following" [23]:

- €350,000
- 2% of the average amount of the reserve assets
- a quarter of the fixed overheads of the preceding year;

In addition to MICAR the European Banking Authority has issued multiple regulatory technical standards (RTS) and established guidelines on asset reserves. The key summary is that the relevant RTS states, that a stablecoin issuer should have an amount of 3% of the average amount of the reserve assets. More details are available here: [6].

7.3.8 Redemption

The issuers may be expected to specify and disclose that all the holders of its stablecoin would have a direct legal right to redeem the stablecoins for the pegged currency at par value and that redemption requests can be made at any time with the issuer. Any conditions that the issuer wishes to impose for redemptions, such as fees and minimum redemption amount, and any other communication channels with the public regarding handling of its stablecoins.

Issuers should return the par value of the stablecoin to the holder, guaranteeing a timely redemption. A redemption request is generally deemed as legitimate if the holder of the coins can meet the issuer's onboarding requirements, including the applicable customer onboarding rules to mitigate ML/TF risks. To protect consumers or where it is in the interest of the public, regulators will exercise its powers as needed, such as directing the issuer to liquidate the pool assets within an appropriate specified period.

7.3.9 Disclosure

Issuers may be also required to publish a white paper containing details which will include description of coins, expected use cases, rights and obligations related to the token of the issuers as well as holders as well as risks that can affect the stability of the stablecoin and such information needs to be updated regularly. Also, regulators may be looking for factsheet covering the best practice for the holders to be published by the issuer.

7.3.10 Transfer time

In general, regulators may be expecting digital assets service providers (which offer the service of arranging the transmission of stablecoins) to complete the transfer from one party to another in no more than five business days from the day the transfer request is received. The purpose is to be in sync with the money transmission requirements as set by different regulators globally. Please see also chapter 8.2.2 “Time to finality”.

8 Blockchain/ DLT Architecture

8.1 Blockchain / DLT candidates

This section provides an unbiased overview of technology and protocols within the crypto space which are candidates for building the technological platform of a stablecoin arrangement. The intention is to highlight technical features without endorsing specific products or vendors. It's important to note that the three technologies which are depicted in the following represent just a **subset** of the numerous options currently under development.

8.1.1 Ethereum based blockchain

The advantages of Ethereum are the large community, the mature tech, and a diverse ecosystem. These aspects position it as a strong candidate for most blockchain/DLT solutions.

For blockchain systems utilizing the Ethereum Virtual Machine (EVM), novel layer-2 solutions have emerged to tackle the scalability aspect of the blockchain trilemma, i.e. the balance between decentralization, security, and scalability. The objective is to ensure that EVM-powered blockchain technology and decentralized applications are universally accessible and cost-effective, at any scale. The basic approach is to process transactions and therefore data computation power out of the main layer-1 chain, on the layer-2 system.

However, the additional layers lead to more complexity as they also need to be integrated. These integration points become critical and require careful management to ensure the overall effectiveness of the security posture.

8.1.2 Hashgraph-Based DLT Protocols

Hashgraph based Distributed Ledger Technology (DLT) takes a different approach to traditional blockchain systems.

One key advantage is its high throughput and speed, offering a faster transaction processing and reduced latencies. Hashgraph based DLTs achieves fast finality for transactions which negates the needs to build a layered blockchain architecture to scale. This scaling aspect is a decisive criterion since a layered DLT architecture could be avoided.

The efficiency of Hashgraph often leads to reduced transaction costs and therefore lower transaction fees.

Compared to EVM blockchains, Hashgraph based DLTs often exhibits a clearer and more explicit segregation between consensus and transaction/state functionalities. The asynchronous Byzantine Fault tolerance (aBFT) consensus mechanism ensures that the

network's security and reliability remains high even if a significant number of nodes are compromised.

Hashgraph's consensus algorithm guarantees fair order of transactions, thus preventing manipulation or censorship.

8.1.3 Bitcoin Lightning

Bitcoin Lightning builds a second layer system on top of the Bitcoin blockchain network and it has the following key advantages:

8.1.3.1 Swift Payments

The Lightning network can handle up to 1 million transactions per second per channel, which represents the connection between two nodes. Transactions can be processed in a matter of milliseconds, resulting in exceptionally rapid payment processing.

8.1.3.2 Cost-Effectiveness

The network is highly cost-effective because it doesn't require payments to miners, as transactions are not executed on the primary Bitcoin network. Transaction costs are exceptionally low, typically around 4-5 Satoshi’s, equivalent to a very small fraction of a Euro according to the current Bitcoin price.

8.1.3.3 Flexibility

Unlike the main Bitcoin network, the Lightning network doesn't necessitate extensive update processes over extended periods. Transactions on the Lightning network involve just two parties who need to reach consensus on the software state, simplifying the process. This architecture makes the network highly adaptable and quick to develop, facilitating easy adjustments. Furthermore, it enables the subdivision of Satoshi’s, allowing for even smaller payments to be processed.

8.1.3.4 New functionality to support stablecoins

The new Taproot assets protocol is building functionality to bring stablecoins and tokenized assets to Bitcoin. Since the Lightning network is Bitcoin’s leading layer 2 and since Bitcoin is the cryptocurrency with the highest market capitalization, this network is a serious option to build the foundation of any stablecoin arrangement.

With the taproot update, the Lightning network enhances the privacy of the Bitcoin main layer, providing greater anonymity for users. However, the inability to reverse transactions likely increases attractiveness to fraudsters and potential launderer and contradicts the requirement of a stablecoin arrangement to comply with regulatory frameworks, which mandate transparency, auditability, and KYB/KYC features.

8.2 Technology and features on the blockchain layer which are relevant for stablecoins

This chapter explores selected features embedded in blockchain layer-1 and DLT systems that significantly influence the usability of stablecoins. The underlying blockchain infrastructure plays a crucial role in determining the efficiency, security, and interoperability of stablecoin transactions. This chapter focuses on several key features of the blockchain layer that directly impact the stablecoin usability.

8.2.1 Identity Protocols for Seamless Transactions

One noteworthy feature of the blockchain layer is the availability of an identity protocol, such as the open-source standard “SocialConnect”[12] (as an example), that enhances the convenience and interoperability of stablecoin transactions. By allowing users to be identified through social indicators like phone numbers or email addresses, platforms enable direct stablecoin transactions to mobile phone numbers, fostering a user-friendly experience.

8.2.2 Time to Finality (TTF)

The performance of a DLT often is determined by the Transactions per Second (TPS) value but the TPS metric does not really reflect the complete view about the efficiency of a DLT.

While TPS measures transaction processing speed, TTF encompasses the entire lifecycle of a transaction, from initiation to irreversible completion within the system. This latter metric is crucial for settlements using stablecoins, as it directly impacts time efficiency. To ensure accurate balance sheet reporting, stablecoin arrangements must clearly define and document settlement finality (see also chapter 6.1.7 Transactional finality):

The settlement finality consists of two aspects:

1. The TTF
2. The confirmation time

The confirmation time reflects the amount of time until a DLT system confirms a transaction. Due to the confirmation process in most cases, several blocks need to be waited upon for finality to be considered acceptable.

Key factors influencing TTF include:

- The consensus mechanism of the DLT
- The network configuration
    - Block time (as the frequency at which new blocks are added)
    - Block propagation time (influences the block time and is about the time blocks are shared across the network)
    - Network latency
    - Number of nodes

8.2.3 Sustainability and scalability

Keeping necessary computing power and therefore carbon emissions at a minimum is an important factor in any blockchain and DLT based solution. For investors, customers and enterprises low carbon emissions are treated as one important factor of a sustainable systems. Regarding EVM based systems the new Proof-of-Stake algorithm is one important step into the right direction, see e.g. [10]. For hashgraph-based DLTs [24] as well as for the Lightning network sustainability aspects are also an important key goal.

Scalability is one important factor for ensuring that blockchain/DLT systems can meet the demands of modern financial transactions. The three technologies mentioned above achieve scalability through their unique characteristics, which are concisely outlined in chapter 8.1.

8.2.4 Transaction fee considerations

Unanticipated spikes in fees pose a significant threat to the widespread availability of the payment service. The size and currency of transaction fees play an important role in stablecoin transactions. Especially for smaller transactions, transaction fee size is crucial.

Additionally, for seamless stablecoin transactions, the blockchain could support the payment of transaction fees in stablecoins. This capability, allowing users to pay gas fees using the same currency as the stablecoin being transacted. With this feature users can transact using the stablecoin without the need for another currency in the wallet.

8.2.5 Uptime and Security

High uptime, approaching 100%, is imperative to ensure constant availability for stablecoin transactions. A reliable and robust blockchain layer contributes to the uninterrupted functionality of stablecoins. Furthermore, the security and immutability of the blockchain layer are paramount, safeguarding stablecoin applications against potential threats and ensuring the integrity of transactional data.

8.2.6 Oracle Design for Stability Mechanism

The role of oracles cannot be overstated in stablecoin ecosystems. Oracles bring off-chain prices, such as foreign exchange rates or fiat currency values, on-chain, influencing the stability mechanism of stablecoins. Depending on the stability mechanism, blockchain networks must possess a robust and reliable oracle infrastructure to support the accurate and timely integration of external price data, thereby reinforcing the stability of the stablecoin.

With the new concept of Decentralized Oracle Networks as presented by Chainlink in their new Whitepaper 2.0 [11] a new generation of oracle networks will be designed using new consensus algorithms established by a committee of nodes. It offers a higher level of trust with additional features, although many of these features are currently visionary and not fully developed. This innovative approach of Decentralized Oracle Networks (DONs), as outlined in Chainlink's latest Whitepaper 2.0 [11], offers also – next to bridging off-chain and on-chain world - proof-of-reserve functionality and the opportunity to serve as a decentralized middleware proxy. With DON enabled proof of reserve - as an example – it is possible to implement cryptocurrency wrapping from a source chain to a target chain.

Another interesting functionality is to use DONs as a middleware layer which abstracts away all the complexities coming with DLT such as gas/transaction fees and chain-reorganisations. In addition, DONs abstract away from specific blockchain or DLT types, and thus is one option for telecoms to connect their legacy enterprise systems to decentralized networks.

8.2.7 Account Abstraction

Since 2023, the concept of "Account abstraction" is available for EVM-based systems. On Ethereum there are two types of accounts: externally owned accounts (EOAs) and contracts

accounts. Only the EOAs are able to initiate transactions. With the feature of “Account Abstraction” contract accounts and EOAs will be unified. The logic of signing transactions is removed from the account by adding an additional abstraction layer around the signing.

The logic around the signing function – preconditions and post-processing – can now be encoded in a wallet, user accounts become ‘programmable’. Thus, features like multi-sig, 2-factor, and authentication functions can be added, which are also important functions for enterprises. It will also provide more flexibility to the development of non-custodial blockchain UI/UX and leverage the mass adoption process.

8.3 Interoperabiltiy and Cross-Chain capabilities

Interoperability emerges as a vital facet, enabling seamless interaction between stablecoins and other applications, wallets, and custody solutions. Blockchain networks adhering to the Ethereum Virtual Machine (EVM) standard, benefit from a thriving ecosystem of builders, fostering the development of interoperable applications and expanding the utility of stablecoins. Interoperability also extends to non-EVM systems such as Hashgraph based DLTs or Bitcoin Lightning.

The future of web3 is shaping up to be multi-chain, with numerous layer-1 blockchains and layer-2 scaling solutions emerging. This proliferation of chains has also led to fragmentation, with users, assets, applications, and liquidity distributed across different networks. While individual chains cater to specific needs, seamless interoperability between them is required to unlock the full capabilities of web3.

The solution lies in cross-chain communication protocols that allow seamless flow of data, tokens, and transactions. Integrated cross-chain infrastructure offers flexibility to users in transferring assets and interacting with applications across different blockchains easily. For stablecoins, integrating with cross-chain bridges ensures speedy, low-cost transfer of tokens across networks. It also enables seamless interoperability across web3 ecosystems relying on different chains, while at the same time supporting greater liquidity and usage of Stablecoin assets.

Cross-chain interoperability protocols will be critical in linking these disparate networks into a unified ecosystem. Stablecoin projects should prioritize compatibility with leading bridge protocols to enable frictionless cross-chain transactions and drive adoption across fragmented web3 networks.

8.4 High-level solution approach

8.4.1 The operating model

The operating model for a settlement application can be summarised into the following general use case groups, which can modularly be enabled market by market:

1. Digital Asset Wallet (to hold/deposit/withdraw stablecoins and other digital assets)
2. Direct fiat rails/payments to/from digital assets (to deposit, withdraw and optionally connected to domestic mobile wallet run by an operator)
3. Trade/Swap between stablecoins

4. Transfer/Send stablecoins to other wallets (optionally to external wallets)

8.4.2 The building blocks

The following graphic shows the building blocks of any stablecoin solution.

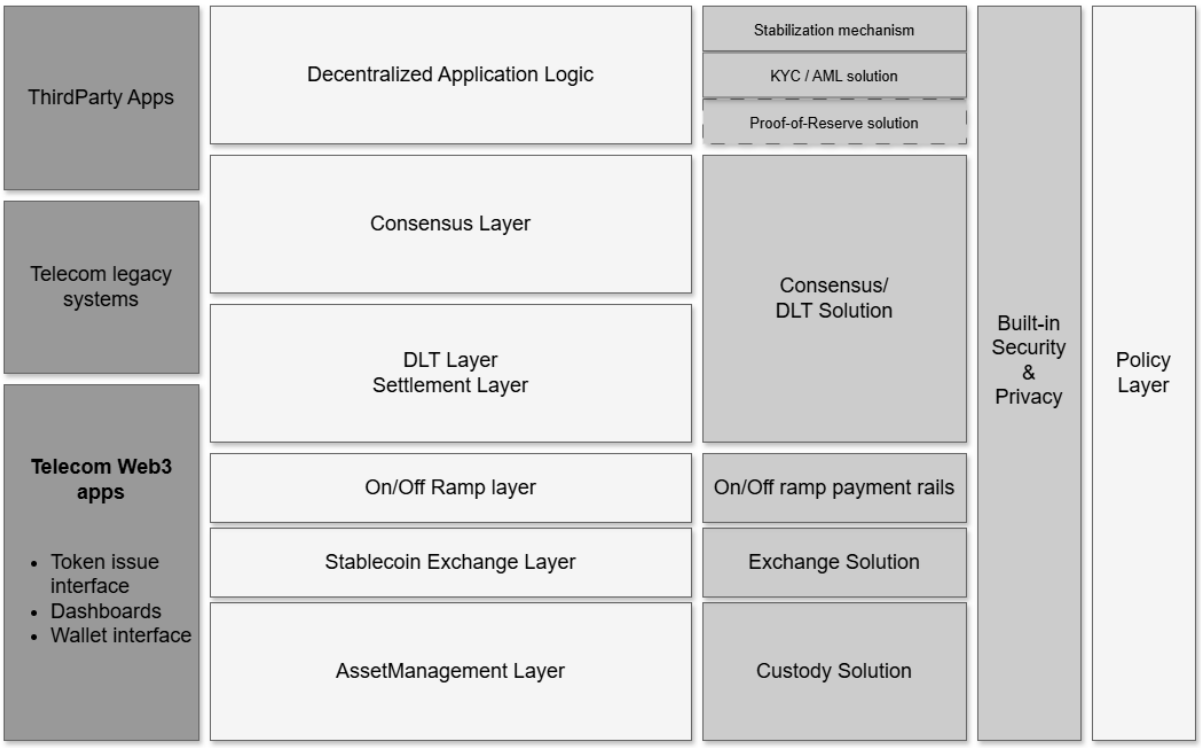


Figure 8.4.2.1 The building blocks of a stablecoin arrangement

The *Asset Management layer*'s responsibility is to store, maintain and protect digital assets (stablecoins) on behalf of telecoms as owners. It will be realized by a custody solution where a custody provider is using an asset management platform.

The *Stablecoin Exchange Layer* provides the ability to swap stablecoins against each other. This is required in a solution where telecoms launch local stablecoins but for cross-border settlements a "global" stablecoin is used.

To be able to convert fiat currencies into crypto currencies *On/off ramp payment rails* are needed. One core function is to determine the appropriate exchange rate to convert stablecoins into the relevant fiat currency and vice versa.

The *DLT and consensus layer* build the stablecoin payment solution whereas consensus and transactional layer are logical separated. In some DLT/blockchain implementations consensus and transactions have a high cohesion whereas in some DLT networks both layers are explicitly isolated.

The *Decentralized application logic* determines the algorithms regarding the supply and demand of the stablecoins, the access roles and security rules and in general the behaviour and properties of a stablecoin. The business logic also defines the KYC/AML rules and in case of backed stablecoins a proof-of-reserve integration.

The consuming applications are web applications which build the integration into the telecom Business Support Systems (BSS). The BSS is the system within a telecom where business and/or customer-facing functionality, Customer Relationship Management (CRM), Billing and rating as well as cross-carrier transaction functionality are located. These applications - on the left side of the graphic – communicate to the different layers through APIs.

For each building block and involved components policies exist. The implementation of each component and APIs should follow the privacy- and-security-by-design principles.

All the mentioned building blocks are conceptual and need to be implemented by concrete solutions. As examples, regarding the application logic different natural languages exist to implement smart contracts, different DLT networks exist and as exchange solutions centralized and decentralized provider exists. For decentralized exchanges several Automated Market Maker implementations exist, all using different exchange functions.

Telecom providers need to develop a strong technical and professional understanding of decentralized systems to fully capitalize on their potential. Typically, payment processing is a distinct business function that falls outside their primary domain. Therefore, when telecoms decide to enter the area of decentralized finance, it is recommended that they initially use managed services for all the building blocks. Over time, and as part of a continuous evolvement, telecoms may increasingly develop and manage some components on their own.

8.4.3 Integration options

The fast-paced development of blockchain/DL technology creates a challenge for businesses. New blockchains that become increasingly popular with their partners may appear faster than companies can update their current systems to interact with them. This challenge is sometimes referred to as "blockchain agility." It describes the difficulty for businesses to keep up with the evolving landscape of blockchain technologies. Therefore, one integration goal should be to abstract away the complexity which comes with blockchain and DLT and to assure, that the integration points (APIs, data entities) remain stable even when the integrated DLT system changes.

Telecoms have different options to connect to any blockchain/DLT solution. The following list reflects the main integration patterns; however, it is still a subset of options. Options can be mixed, and the “final” architecture can only be formulated, when on the solution-level the concrete used blockchain/DLT systems and vendors have been selected. Then it becomes clear which APIs and integration points are available.

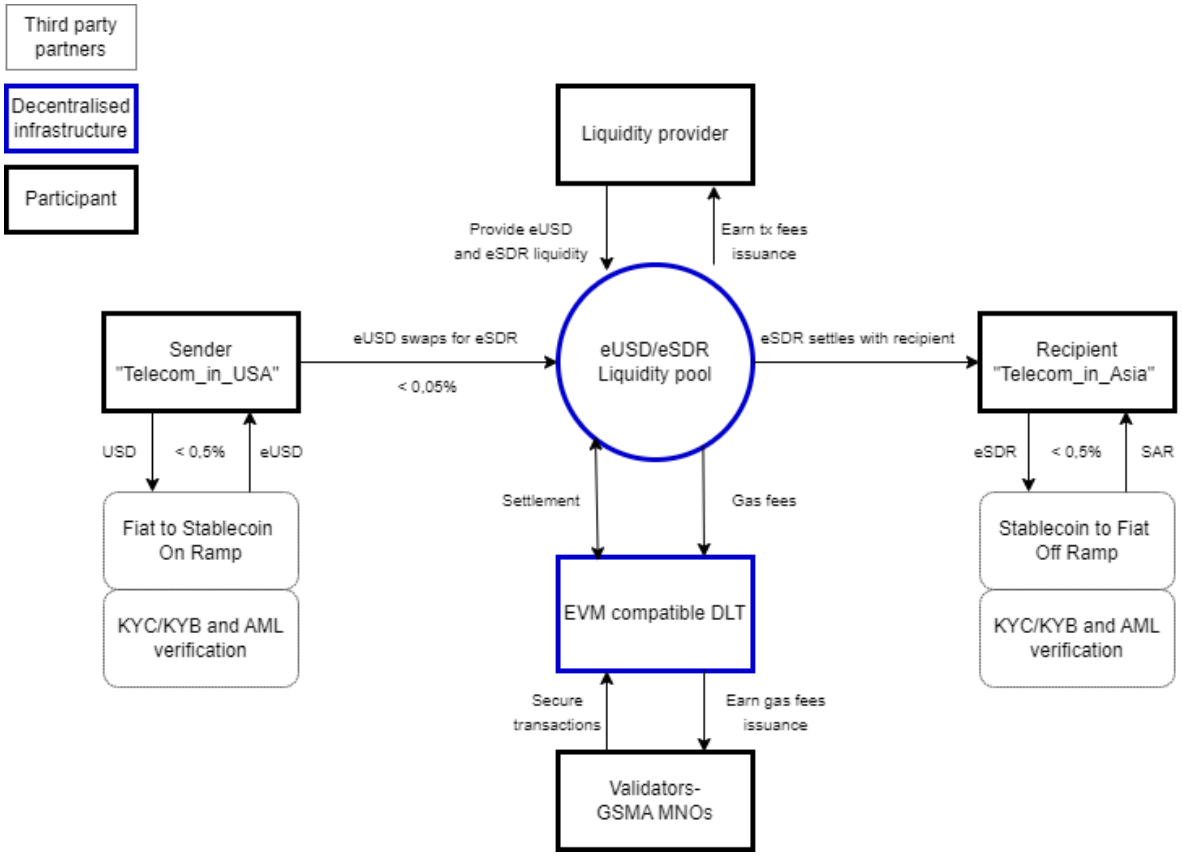
1. Integration using a middleware proxy layer where this layer abstracts away from the blockchain/DLT technologies. This layer can then additionally serve as a security boundary. This layer could be either developed and/or hosted by telecom IT or it will be completely delegated to an external integrator.

2. Integration by using “Decentralized Oracle Networks (DONs)” layer where this layer has mainly the same functionalities and purposes as outlined in option 1.

3. Direct integration from the telecom IT system.

8.4.4 E2E ecosystem architecture

Finally, the graphic below depicts the ecosystem architecture to facilitate end to end settlement between Mobile Network Operators (MNOs).



The scenario illustrated is an example of a settlement transaction between international telecoms. The approach behind this flow is, that the sender does not use the “global” stablecoin directly but first get the stablecoin issued in its jurisdiction and then exchanges that stablecoin using an AMM provider against the stablecoin used for cross-border settlements.

The benefit of having different currency denominated stablecoins by jurisdiction is that it provides the option for the telecoms and partners to hold/have exposure to more than one currency, and that it is easier to have the stablecoin in the respective jurisdiction compliant to the local regulatory framework. However, this approach does increase the complexity, where some sort of Automated market maker/Exchange and different reserves are required.

To start with a solution, it may make sense that at a pilot stage only one stablecoin is used. This would take away the need for a swap engine, from the graph above.

As formulated in chapter “6.3.3 Standardization of a Global Solution” telecoms enjoy economic benefits as they act in different roles. Stablecoin issuance is not shown in the graphic above, but to sum up:

Issuing a stablecoin is a relatively easy business model where very few upfront capital is required. Basically, two options exist:

1. Lending (fractional reserve), which is similar to traditional banking

2. Earn interests on reserves in a fully backed model. Telecoms purchase treasuries and earn yields.

9 Cybersecurity and data privacy measures

Implementing security controls for an enterprise DLT system involves several key considerations to ensure the integrity, confidentiality, and availability of the data and processes. For example, security concerns, such as the potential for smart contract software weaknesses and vulnerabilities [13] which can lead to potential stablecoin theft, can prevent large-scale adoption. Overcoming these concerns is crucial for stablecoins to achieve the adoption needed in the Telco industry. At the same time, security and privacy issues can be overcome with sufficient funding for security and privacy research, community engagement, and industry-wide collaboration. This is true even as new threats and risks will inevitably arise. Security and Privacy by Design must be addressed to ensure a smooth transition to this new structural paradigm for settlements.

A consortium backed DLT platform usually involve three types of organizations.

1) The platform owner (Consortium)

2) The platform operator

3) The members of the platform

The members are companies that have already developed Security Compliance Frameworks, security policies and models. These are often inspired by and derived from specific certification standards, like in Europe the ISO 27001/2 standard, and are then customized for the specifics in the Telecom environment. Any security framework and policies which are created and applied to the platform and their interfaces must be compliant with the security standards of the member's systems. The End-to-End (E2E) security model needs to be designed in such a way to ensure that data is protected throughout its entire journey, from the point of origin to its final destination.

Security controls with respect to an enterprise DLT system can be classified as follows:

- Security controls that are specific to DLT/blockchain technology
- Conventional security controls
- Controls required for regulatory compliance

Security controls, that are specific to enterprise DLT solutions, should cover:

- Identity and authentication measures: Use strong, multi-factor authentication to verify the identities of users and nodes
- Key/ Wallet management
- Network access management/ Authorization: Implementing role-based access control to ensure users have the minimum necessary permissions.
- Secure Network Communication (specific to inter-node communication)

- Data privacy
- Smart contract security
    - Code Audits for vulnerability management and best practice
    - Formal verification/methods to prove correctness
- Consensus Mechanism, Fork management
    - Byzantine Fault Tolerance – tolerance for malicious nodes
    - Regular updates to keep consensus algorithms and software up to date to protect against known vulnerabilities
- Cross-chain extension points

Conventional security controls include:

- Network security
    - Firewall and Intrusion Detection Systems to protect the network from unauthorized access and monitor for suspicious activities.
    - Secure Communication Protocols to secure communication between nodes.
- Hardening of the system components and software
- Data Integrity and Confidentiality
    - Encryption: Encrypt data at rest and in transit to protect against unauthorized access
    - Hashing: Use cryptographic hashing to ensure data integrity and detect any unauthorized changes
- Audit, Logging and Monitoring with event notification
    - Realtime monitoring to continuously monitor the DLT network for anomalies and potential security breaches
    - Comprehensive Logging to maintain detailed logs of all transactions and access events for audit purposes
- Incident Response and Recovery
    - Incident Response Plan to quickly address security breaches
    - Backup and Recovery to ensure data can be restored in case of failure
- Compliance and Governance

  - Regulatory compliance to ensure DLT system complies with relevant regulations and standards
  - Governance Framework to oversee the security policies and procedures.

- Decommissioning

In general, the top management (Executive committee) of every company is responsible for ensuring that all business units function properly, that risks are logged and tracked to closure. Information and cybersecurity controls are enablers of these business functions. With respect to an enterprise DLT platform, this means, that two groups of the management level are involved:

1. The management of the consortium which owns and/or operates the platform
2. The management of the members that approves participation in the platform

The management must initiate, control and monitor the security process. Moreover, management should enable the provision of resources for information security. In general, the members of the consortium need to create a governance structure to steer security processes.

10 Standardization of Stablecoins in Telecom Industry

The integration of stablecoins within the telecommunications industry could emerge as a groundbreaking development in the financial and technological landscape. As these digital assets gain prominence as a means of facilitating micropayments, cross-border transactions, and various telecom-related services, the need for standardization becomes increasingly evident and it should aim to ensure interoperability, security, and regulatory compliance.

Candidates for standardization are:

- Processes like onboarding, KYB, KYC, in general the handling of all related processes within a stablecoin arrangement
- Technological components like APIs, operations, and data entities. These build the access points for services like Asset Management, Custody, etc (see building blocks as depicted in chapter 8.4.2)
- DLT technological standards
- Align with international standards as proposed by the G20 cross-border payments programme (BIS (2020)). “The G20 cross-border payments programme contains building blocks 14 (on harmonisation of ISO 20022) and 15 (on harmonisation of API protocols). These building blocks will cover crypto and stablecoin compatibility with ISO 20022, and adoption of API standards by SAs, particularly for on- and off-ramps [5]

The success of a standardization initiative will depend on collaboration among industry stakeholders, regulators, and standard-setting bodies to create a cohesive and sustainable framework for the use of stablecoins within the telecommunications industry.

11 Outlook

Across industries, it's clear that the versatility of stablecoins extends beyond the realm of financial transactions for telcos. These digital assets can be utilized for a variety of purposes including loyalty programs, incentive schemes, and even customer rewards. For example, there is potential to use stablecoins to enable automated payments with concepts such as non-fungible tokens (NFTs) or in the Metaverse. As the market share for digital assets continues to grow, forecast to reach $56.4 million in annual revenue in 2023 and 994 million users by 2027 [14], it makes sense for telcos to explore creative ways to integrate stablecoins into their business models. This further foster customer engagement and loyalty while reducing the operational costs associated with similar customer loyalty and digital asset products utilizing mainstream technology.

The World Bank classifies 1.4 billion people globally as 'unbanked' (based on an analysis for the year 2021) [19] but recognizes that digital financial services signal a reduction in this figure. Around 18% of the global population have limited or no access to financial infrastructure to facilitate easy payments or other financial services. Stablecoins represent financial inclusion for this segment of the world's population, providing access to digital financial services for individuals and entities excluded from traditional banking systems. The only barrier to entry is the need for access to a smartphone. In regions with limited access to banking infrastructure, telcos can use stablecoins to think innovatively regarding the financial solutions they are providing. In turn, this can help, foster economic growth globally.

We believe stablecoins, and more generally tokenization (see section 11.5), have potential applications in the following domains:

11.1 Metaverse

Telecoms can provide reliable and high-speed connectivity to users and businesses in the virtual space of the Metaverse. This infrastructure can be monetized through service subscriptions and data plans. Telecoms could enter content delivery partnerships or acquire virtual content providers to deliver a wide array of digital content, such as music, movies, virtual experiences, and educational materials. Revenue can be generated through for example content subscriptions, pay-per-view models, and advertising.

11.2 Roaming

The potential of stablecoins in roaming services lies particularly in the simplification for both established and new players in the roaming system, the transparency of transactions and the cost pressure in this area. Roaming requires continuous billing between providers. Depending on which network a customer is logged into, the customer's provider must pay a fee for using the third-party network. Given the large number of existing providers and their roaming contracts with each other, this results in a very high number of transactions that must be automated and trustworthy.

11.3 6G

6G, expected to debut around 2030, is envisioned to be ubiquitous and redefine the telecommunications landscape. With the capability to offer connectivity not just through radio frequencies but also via satellite and WiFi, it represents a transformative shift in the industry. Due to the diverse array of technologies that 6G leverages, an increasing number of

systems are required to represent each respective technology. Stablecoins could serve as incentives for expanding network coverage into remote or underserved areas. By facilitating microtransactions for connectivity services, they encourage telecom operators to reach regions previously deemed uneconomical.

11.4 IOT and IIOT

Most of the MNOs already have IOT solutions in place. These solutions are based on a centralized setup, using centralized security, and are integrated into the BSS and OSS landscape. Often MNOs use centralized IOT Platform capabilities and cloud architectures where a central hub controls the data and signal flow. With Web3 and DLT decentralized networks come into play. The main promises are:

- DLT solutions build trust in (I)IoT data by tracking provenance, proofs and permissions
- DLT secures the data, provides OOTB digital identity, eliminating "single point of failure"
- DLT enables automated payments (using crypto currencies)

If using DLT, payment solutions are already an out-of-the-box built-in capability of a DLT, then in contrast, a centralized approach and tokenization/payment without underlying DLT comes with structural weaknesses. Such as the need to layer application programming interfaces (APIs). Without DLT each of the above-mentioned features must be built from scratch and requires explicit integration, which increases the complexity of the solution.

Distributed Ledger Technology (DLT) and blockchain have a transformative potential for cyber-physical systems. It can build the foundation of a new type of machine economy [15].

By using stablecoins telecoms could develop new pay-per-use services. Telecoms could engage in new production and supply chain models. In the context of the renewable energy domain the traceability of energy consumptions patterns enables the reward and incentivisation of the use of machines [15].

In order to build a trusted system every machine and device in a decentralized I(I)oT network requires a connector which ties together the physical and cyber parts of the “cyber physical system”. This connector may be called a trusted anchor [15] which enables the trust by applying a reliable incorruptible identity to the machine. This connector component is a physical device, embedded into the machine or device, which consists of a hardware wallet and a Secure Element. Additionally, telecom companies like Vodafone are exploring ways to create a reliable foundation for a reliable identity. One approach they're considering involves embedding cryptocurrency wallets directly into SIM cards, which could potentially serve as a trusted anchor for the system [16].

The trusted anchor has two main responsibilities

- Creating a non-questionable identity and linking the produced output (data and signals) to this identity
- Enable tokenization of the output data by using cryptographical functions in real time

The trusted anchor is a core component of the trust management and an enabler for building a sustainable economic model since all machine work, it’s algorithms and produced output becomes reliable and thus, valuable.

11.5 Stablecoins and tokenization

In a general sense, "tokenization" refers to the process of representing underlying assets or rights from the real-world on a DLT system as digital tokens. These tokens can then be traded on the DLT network. Access to the token means typically having ownership of the underlying asset: Tokenisation refers to the process of representing claims. Real-world assets from the telecommunications sector can be any unit of content, any object in the metaverse, network resources, network usage, (I)IOT machine signals and data, etc.

Stablecoins, on the other hand, are a specific type of cryptocurrency. Although one key characteristic is, that they aim to provide a stable value by pegging to a real word asset (among other things to a currency or commodity), they do not represent the peg. They promise that every holder of a stablecoin will get the pegged value at par, but it is not a representation in the sense of a digital token. In addition, stablecoins adhere closely and only to the use case of payment and stablecoins are typically used as a medium of exchange, a unit of account, or a store of value in digital transactions.

One key difference between a digital token and stablecoin is ability to support the “Singleness of money”. Private tokenised money that circulate as bearer instruments, like stablecoins, may entail departures in their relative exchange values away from par in violation of the “singleness of money” [17]. However, using a well-designed stabilization mechanism, stablecoins could become a reliable and universally accepted store of value, unit of account, and medium of exchange, effectively approaching the ideal of singleness of money.

12 Conclusion

Telecom operators have a significant advantage: a large and established customer base with a certain level of trust. This trust stems from the nature of telecom services – long-term contracts ensure constant relationships, making them essential for most users. Smartphones, a constant companion for many customers, further underpins this connection. The daily use of apps fosters an implicit, personal relationship between users and the underlying telecom infrastructure – and by extension, the operators who provide it.

This trusted relationship is a great enabler to introduce a new area of services, and these are trustless decentralized and crypto economic services based on stablecoins.

Telecoms might follow a phased approach until they reach the level of proven trust-minimized applications and services where stablecoins are integrated as a store of value and medium of exchange. A possible starting point could be a wholesale settlement use case, where a stablecoin is used as the payment method within a limited partner network. This controlled environment allows telecoms to gain experience and build confidence before venturing into more complex applications. By implementing the "Wholesale settlement" use case as the initial step, telecoms can also directly benefit from cost reduction.

Other use cases will follow. Each telecom operator and provider will have the flexibility to launch their own services and potentially even cryptocurrencies by leveraging integration points within the initial system.

Telecom operators will have the autonomy to choose the technical platform that best aligns with their specific needs and infrastructure. Web3 is envisioned as an interconnected ecosystem of networks, where seamless interoperability will be a key feature. Each decentralized network will likely specialize in a particular area or use case, contributing to a broader, interconnected world of trust minimized applications and services. The integration points can be native bridges or DONs. DONs or equivalent oracle networks enable more use cases like “Proof of reserves management”, “Digital Identity services”, privacy enabled payment services or other use cases which require a bridge to the off-chain world.

The integration of local stablecoins within individual jurisdictions is also a key consideration. A critical decision needs to be made before a Minimum Viable Product (MVP) can be initiated: should there be a new, dedicated industry stablecoin from the beginning, or shall there be an existing stablecoin solution used?

The outcome of this decision will also depend on the amount of telecom operators which are willing to invest in such a solution. Launching a new stablecoin offers a more direct path towards the goal – a dedicated "Telecom Industry Stablecoin." This approach minimizes the need for future adjustments and refactoring efforts but requires a significant upfront investment. Conversely, leveraging an existing stablecoin provides a faster route to the initial milestone – a functioning wholesale settlement solution.

We've already explored the benefits of stablecoins. However, the concept of tokenization offers an even broader range of applications. Unlike stablecoins with their focus on being a means of payment and medium of exchange, tokenization can be applied to various usages and fields like the Metaverse, Industrial IoT (IIOT), and network usage. To delve deeper into this potential, a dedicated paper on the use cases of tokenization will follow.

12.1 Recommendations

In this section the initial steps and activities are listed to start building the stablecoin Arrangement (as a MVP). GSMA could advise and support the process.

- Governance
    - Creation of a network with interested parties from the telecommunication sector for a stablecoin MVP solution. This partner network takes responsibility for all below mentioned activities.
    - Decide on the scope of the MVP. As a recommended use case a wholesale settlement use case should be used
    - This use case can have integration points into the telecom IT landscape, when the settlement is integrated into a concrete use case, i.e. Roaming
    - Establish an initial governance process to manage the MVP scope.

- Capability
  - Develop the organisational capability to manage the MVP
    - Funding
    - Provision of human resources
  - Support education and training programs to increase understanding of the new legal, operational, and technological aspects of a stablecoin.
- Stablecoin design
  - As part of the MVP fundamental decisions should be made. Decisions include:
    - Selection of the DLT platform
    - Design of the peg currency (or basket of currencies)
    - Selection of the concrete providers of the building blocks of the stablecoin arrangement (see chapter 8.4.2)
      - i.e., on- and off-ramp rails
      - Wallets
      - Custody providers etc
- Regulatory compliance
  - Decision on the location (jurisdiction) of the specific entities of the stablecoin arrangement (see chapter 8.4.2)
  - Decision on the to be included jurisdictions.
- IT-Design
  - Start developing a global API to build an abstraction layer to integrate telecom IT and the Stablecoin arrangement services.

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	January 2025	This is the version for approval	GSMA	Christian Schepp, Vodafone

A.2 Other Information

Type	Description
Document Owner	GSMA
Contributors / Company	Shamit Bhat GSMA (Services)

	Gareth Williams GSMA Karoline Döhring Vodafone Markus Franke Mentolabs Richard MacNamara Zain Monique Morrow Hedera Ricardo Pires Telcoin Rajesh Sabari Telcoin Christian Schepp Vodafone Greg Scullard Swirldslabs

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.