GBBC
Global Blockchain
Business Council

DIGITAL MONEY & PAYMENTS REPORT

GLOBAL STANDARDS MAPPING INITIATIVE 6.0

DIGITAL MONEY & PAYMENTS: PATH TOWARD CONVERGENCE BETWEEN LEDGER-BASED AND TRADITIONAL SYSTEMS

GBBC GSMI 6.0

GLOBAL BLOCKCHAIN BUSINESS COUNCIL

DC Location:
1629 K St. NW, Suite 300
Washington, DC 20006

Geneva Location:
Rue de Lyon 42B
1203 Geneva
Switzerland

For the purposes of this paper, 'blockchain-based digital money' refers to a subset of digital currencies: stablecoins, CBDCs, and deposit tokens, whose issuance, transfer, and record-keeping rely on distributed ledger technology (DLT) or blockchain rails.

INTRODUCTION

Digital money encompasses a broad spectrum of models, ranging from private issuance to sovereign issuance, deployed across both traditional banking and DLT rails, over public and private blockchains. We start with a basic taxonomy defining the range of models of digital money that this paper will focus on, and they differentiate themselves. This paper focuses on a specific subset of blockchain-based digital money models, specifically those that are backed by assets in a regulatory compliant manner, with the objective of explaining digital money payments using traditional payment processing frameworks.

Taxonomy of Digital Money Models: We start with an overview of the digital money models under the scope of this paper, their: stablecoins, central bank digital currencies (CBDCs), and deposit tokens. We cover the opportunities of each, use cases, and challenges that need to be addressed for scale.

Ecosystem View of Digital Money: Next we cover the ecosystem of key stakeholders and their interactions for payments with stablecoins, CBDCs, and deposit tokens. While they present different starting points from traditional systems by operating on DLT infrastructures, once all regulations and risk management measures are put into place, both ledger-based and traditional payments models start to converge.

Value Chain of Payments with Digital Money: We build on the ecosystem view by illustrating a blueprint of payments using standards in the context of existing payment processes along the value chain.

- We provide an end-to-end view of payment processes mapped out against regulations and standards (both for payments and for blockchain/digital assets)
- We provide a parallel end-to-end view of payment processes mapped out against new considerations for blockchain-based digital money, and any gaps in regulations and standards
- We expect that as standards and regulatory requirements continue to develop, existing gaps will be addressed, and the blockchain-based digital money payments space will continue to converge with the traditional payments structures and approaches

Regulations: Finally, we discuss the case of global stablecoins, CBDCs, and deposit tokens in light of regulatory developments.

As digital money introduces novel issues with the use of blockchain technology and decentralized ledgers, this paper focuses on themes specific to blockchain-based digital money models and their use for payments. These themes in general should apply equally regardless of whether digital money operates on public or private blockchain networks, or if it takes the form of stablecoins, CBDCs, or deposit tokens. This leads us to conclude with open questions and recommendations to achieve scalability for these digital money models that point to the future of ledger-based payment systems.

I) TAXONOMY OF DIGITAL MONEY MODELS

While digital money on blockchain rails[1] may vary widely in its design and incentives – from privately issued representations of fiat currency in the form of stablecoins, to tokenized representations of central bank-issued money, or purely decentralized cryptocurrencies issued by the networks on which they operate – this paper focuses on payments operations, and thus the scope of digital money covered by the following discussion includes solely models that are backed by assets in a regulatory compliant manner. This paper focuses on a specific subset of blockchain-based digital money models: stablecoins, CBDCs, and deposit tokens. Below is an overview of each, illustrating the benefits, opportunities for usage, and challenges to scale.

I.I) STABLECOINS

Most recently, there has been a surge in stablecoin popularity as a form of digital money.

SELECTED DEFINITIONS

- **CFTC (GMAC - DAMS):** Privately-issued, money-like, digital token that aims to maintain a stable value relative to a peg specified by a reference asset(s) and designed to minimize value fluctuations relative to these reference assets(s). They are not issued by a central bank. They must also be at least fully backed by one or more assets specified under the specific regulatory framework, including:

    a. Cash: to one or a combination of fiat currencies
    b. Securities: low risk, highly liquid securities such as those classified as High-Quality-Liquid Assets ("HQLA") under the BCBS LCR30 framework (e.g., US Treasury Bills)

- **Financial Stability Board (FSB):** The FSB considers that so-called stablecoins are a type of crypto-asset 'that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets to other assets.'

- **International Securities Services Association (ISSA):** A class of crypto-currency designed to eliminate the price volatility of cryptocurrencies by backing them with real assets, fiat currencies or a mixture of both. A stablecoin whose price reference is the US Dollar, for example, would be backed 1:1 by US Dollars in a custody account. Investors redeeming the stablecoin would receive one US Dollar for each stablecoin.

- **US GENIUS Act:** The term "payment stablecoin"—(A) means a digital asset— (i) that is or is designed to be used as a means of payment or settlement; and (ii) the issuer of which— (I) is obligated to convert, redeem, or repurchase for a fixed amount of monetary value; and (II) represents it will maintain or creates the reasonable expectation that it will maintain a stable value relative to the value of a fixed amount of monetary value; and (B) that is not— (i) a national currency; or (ii) a security issued by an investment company registered under section 8(a) of the Investment Company Act of 1940 (15 U.S.C. 80a–8(a))

Examples	Description	Market Size (Market Cap)[37]
USDT	Stablecoin – USD backed	$184.5B
USDC	Stablecoin – USD backed	$75.8B
RLUSD	Stablecoin – USD backed	$1.2B
EURC	Stablecoin – EUR backed	$327.3M

STABLECOIN USE CASES

- Facilitate payments as digital money, with less volatility and over more efficient blockchain infrastructure
- Facilitate remittances at lower costs and greater efficiency to move money across borders
- Used in Decentralized Finance (DeFi) to lend, borrow, trade, and liquidity provision (where many stablecoin deposits also earn yield)
- Used as a bridge between crypto & traditional finance (e.g., crypto traders going in and out of trades without having to go back & forth between the traditional banking system & crypto rails)
- Hedge against crypto market swings
- Retail & emerging markets can use stablecoins as an alternative to unstable local currencies, and for small/micro p2p transactions as an alternative to slow or expensive banking services
- Institutional & TradFi benefits in treasury functions

STABLECOIN GROWTH TRENDS

- **Increasing total supply & market cap:** $300B in supply, with strong yearly growth projections (50% or above)[2]
- **Active addresses/users increased** from 19.6M to 30M (Feb 2024-Feb 2025)[3]
- **Monthly transfer volume increased** from 1.9T to 3.9T (Feb 2024-Feb 2025)[4]
- **USD-pegged stablecoins dominate**, with 99% of market share[5], with USDT ($186.67B market cap) & USDC ($76.54B market cap) as clear leaders.[6] USDC is growing faster and may surpass USDT by 2030[7]
- **Regulatory developments are boosting confidence**, as key enabler driving adoption
- **Regulatory developments perceived as a green light for expansion:** For instance, the US GENIUS Act authorizes banks and other institutions to issue stablecoins backed by fiat or high-quality collateral. Institutional adoption has advanced, with stablecoin adoption for activities such as treasury operations, corporate cash management, and overall integration with traditional finance.

STABLECOIN CHALLENGES FOR SCALE

- Regulatory uncertainty remains, as gaps remain across jurisdictions
- Peg stability & reserve transparency are key. If this comes into question, the peg can be broken and erode trust
- Counterparty & network risks if stablecoin issuer or custodian has poor quality assets, risk exposures, and poor governance
- CBDCs in certain jurisdictions may compete with stablecoins
- Stablecoins may pull capital out of banking system in emerging markets where they're perceived as safer value storage alternative

I.II) CENTRAL BANK DIGITAL CURRENCIES (CBDC)

Pilots and prototypes have arisen around the world for several models of CBDC, with a few full launches to date, signaling that many nations perceive CBDCs as a strategic infrastructure. A wide range of design models (retail vs wholesale, offline vs online, account-based vs token-based) can be implemented with various approaches and priorities. When it comes to CBDCs and overall framing of how digital money is used with them, a critical differentiation is retail vs. wholesale. These have significant differences functionally, target user-base wise, regulation-wise, and in terms of adoption and market size. Much of the initial CBDC infrastructure being rolled out, in terms of size, function, and initial adoption, is expected to be at the wholesale level (e.g., largescale settlements between central banks and institutions), where the value proposition focuses more on instant settlement, ledger transparency, reduced costs of moving funds, etc., without the retail-level concerns about privacy in day-to-day transactions.

SELECTED DEFINITIONS

- **Bank of England:** Central bank digital currency (CBDC) is money that a country's central bank can issue. It's called digital (or electronic) because it isn't physical money like notes and coins. It is in the form of an amount on a computer or similar device.
- **CFTC (GMAC - DAMS):** digital tokens representing a claim on a central bank for a fixed amount of central bank money denominated in a single currency; also, a liability of a central bank, with no credit or liquidity risk. It may or may not be programmable.

    a. "General Purpose" or "Retail" CBDC: a CBDC that is specifically designed for use in transactions and holdings by individuals and/or small and medium-sized enterprises;
    b. "Wholesale" CBDC: a CBDC that is specifically designed for wholesale use in transactions and holdings by regulated financial institutions and could be used in the facilitation of regular financial markets functions (e.g., settlement of securities transactions).

- **International Organization for Standardization (ISO):** A CBDC is a digital payment instrument, denominated in the national unit of account, that is a direct liability of the central bank.
- **International Monetary Fund (IMF):** Potentially a new form of digital central bank money that can be distinguished from reserves or settlement balances held by commercial banks at central banks. It is a central bank liability, denominated in an existing unit of account, which serves both as a medium of exchange and a store of value. CBDCs are not cryptoassets.

- **International Securities Services Association (ISSA):** In broad terms, a CBDC is simply a new form of digital liability of a central bank. Because it is issued by a central bank, CBDC is typically thought of as being denominated in the currency of that central bank.
- **National Institute of Standards and Technology (NIST):** Central bank digital currencies (CBDC)… would represent central bank reserves, for reasons such as reinforcing the transmission of monetary policies, establishing new transmission channels, or just in response to a decline in cash.

Examples	Jurisdiction	Description	Market Size (Funds in Circulation)
SandDollar	Bahamas	CBDC - retail	$2.1M in circulation (March 2024 – Central bank statistics)
eNaira	Nigeria	CBDC - retail	$9.16M in circulation (Jan 2025 – Central Bank statistics)
JAM-DEX	Jamaica	CBDC - retail	J$ 257M in circulation (Feb 2023 – central bank statistics)

CBDC USE CASES

- Retail payments, ranging from instant peer-to-peer payments (e.g., phone-to-phone transfers), merchant payments with lower fees and faster settlement, micropayments (e.g., streaming services, per-use digital goods and pay-per-article consent), and even offline payments functionalities.
- Government and public sector innovation, improving the efficiency, transparency, and delivery of public services including government-to-person payments (e.g., social benefits, stimulus checks, disaster relief), tax collection and automatic remittances, delivery of subsidies and grants. CBDCs allow programmable disbursements tied to specific conditions.
- Modernization of payments systems with 24/7 instant and programmable settlement across banks and payment providers, automated reconciliation between financial institutions, and greater reliability.
- Cross-border payments with open and interoperable rails, direct FX settlements between countries, instant trade settlement, real-time fund flows at lower costs, and multi-CBDC platforms reducing layers of correspondent banking processes, and improved compliance with harmonized AML/KYC
- Capital markets modernization, especially for wholesale financial market innovations, allowing tokenized asset settlement, atomic settlement, better intraday liquidity management solutions, and programmable treasury operations. CBCDs support digital asset and tokenized economies
- Monetary policy and macro financial tools for central banks, to be used cautiously, with opportunities for direct transmission of monetary policy, interest-bearing CBDCs as a policy tool, and programmable incentives (e.g., stimulus with expiration dates). All these tools can also provide economic data for macro analysis.
- Cash replacement or complement in societies with declining cash use

CBDC GROWTH TRENDS

- **137 countries and currency unions** (representing 98% of global GDP) have explored CBDCs, with 3 launches, 49 pilots, 20 models in development, and 36 models in research stages[8]
- **Approximately 94% of central banks are actively exploring CBDCs,** according to survey results from the Bank for International Settlements (BIS)[9]
- **34% of central banks now expect to issue a CBDC within the next 3-5 years**, up from 26% a year earlier[10]
- **Payments value using CBDCs** is projected to surpass **USD $200 billion by 2030**
- **Transaction volumes** for the retail pilot of China's digital yuan (e-CNY) reached **RMB 7 trillion** (USD $986 billion) in June 2024 across 17 provinces[11]

CBDC CHALLENGES

- Privacy and civil liberty concerns arise when trying to balance transaction-level visibility for compliance purposes with individual privacy protections (e.g., how to maintain cash-like anonymity while preventing illicit finance), with the risk of government surveillance or overreach.
- Cybersecurity and Operational risks (e.g., fraud, double-spending, counterfeiting), where CBDCs can become a target for nation-state level cyberattacks, make the need for extremely robust, quantum-resilient, and continuously updated security systems imperative. Attacking the infrastructure of a CBDC system can lead to financial instability.
- While many central banks are exploring CBDCs, there are very few actual full launches remain few. The vast majority of implementations are in the form of pilots and prototypes. The lack of live examples can be a hindrance to scalability.
- Retail CBDC models face significant barriers for widespread adoption and usage with respect to updates needed in infrastructure, regulation, and user behavior.
- Given the wide range of CBDC designs, comparability becomes complex
- The rollout of CBDC launches has been slowed among major economies due to various concerns including geopolitical, regulatory, privacy, and financial stability uncertainties.

DEPOSIT TOKENS

Increasing opportunities with deposit tokens arise to bridge traditional banking and digital assets, as they combine legal clarity of traditional banking with the programmability and interoperability of blockchain networks. As on-chain representations of bank deposits, these instruments are subject to the same standards as traditional bank deposits. Blockchain Deposit Accounts by J.P. Morgan's Kinexys is a prominent early example of a blockchain based bank deposit, while JPM Coin is an example of a deposit token.

SELECTED DEFINITIONS

- **CFTC (GMAC - DAMS):** Deposit Tokens - transferable digital tokens issued by a licensed depository institution which evidence a deposit claim against the token-issuing bank or depository institution, for fixed amount of commercial bank money or fiat cash denominated in a single currency.
- **CFTC (GMAC - DAMS):** Tokenized Deposits - digital tokens that represent an existing record of a traditional ownership claim for a bank deposit on the token-issuing bank or depository institution, for a fixed amount of commercial bank money denominated in a single currency.
- **JP Morgan:** Blockchain-based deposits, i.e., distributed ledger-based deposits issued by a licensed depository institution, including deposit tokens, which are forms of commercial bank money.[12]
- **KPMG:** Tokenization of commercial bank money can be in the form of tokenized deposits or deposit tokens. Tokenized deposits are token representation of the commercial deposits where each token is backed by retail or institutional deposits. Whereas a deposit token is the native token on blockchain which directly represents the retail or institutional deposits in form of tokens.[13]

Examples	Description	Transaction Volume
Blockchain Deposit Accounts - Kinexys by JP Morgan	Blockchain Deposit Accounts on private permissioned blockchain (sometimes referred to as a tokenized deposit)	~$5B USD daily Launched in 2019
JPM Coin (JPMD) - Kinexys by JP Morgan	Deposit Token on public blockchain	Launched in Nov 2025

DEPOSIT TOKEN USE CASES

- Instant and programmable payments, enabling instant settlement with embedded logic. This can be beneficial for automated B2B payments, escrowless real estate transfers, automated recurring transfers (e.g., on-chain payroll), and programmable payments. Because deposit tokens can support high volume digital commerce, they can support the scalability of Web3 commerce and a variety of transaction forms at scale, including merchant and retail commerce, and supply chain and trade finance payments.
- Tokenized asset settlement can benefit from a reliable cash with deposit tokens, minimizing counterparty and settlement risks, while reducing capital requirements. This can be beneficial for bond, equity, and fund tokenization, trading of tokenized real-world assets (RWA), atomic settlement of digital securities, repo and securities lending with instant collateral movement, and FX settlement against tokenized currencies or deposits.
- Institutional DeFi, where deposit tokens provide a safe money leg within permissioned DeFi protocols that have passed KYC checks. This allows for a regulated version of solutions like institutional liquidity pools (e.g., FX, lending, repo), automated market makers (AMMs) for wholesale players, credit lines and collateralization based on smart contracts, and on-chain derivatives and structured products
- Automated treasury and management, where corporates can utilize deposit tokens to optimize liquidity, reduce trapped capital, and streamline a range of financial operations with smart contracts, such as 24/7 treasury sweeps, working capital, reconciliations and ERP integrations, and instant transfers across subsidiaries or groups within an organization.
- Interoperability, where deposit tokens can operate as a regulated and bank-issued component of a multi-rail digital money ecosystem, bridging stablecoins with traditional finance, cash instruments across various chains, wholesale settlement across networks, and providing a settlement layer for mixed CBDC and deposit token systems.

DEPOSIT TOKEN GROWTH TRENDS

- **Increased interest and pilots from institutions and banks**, with active experimentations of deposit token uses in areas like cross-border payments, conditional settlements, and yield optimization
- **Growing recognition of opportunities for deposit tokens** as a bridge between traditional banking and digital asset ecosystems
- **Increasing momentum of adoption alongside broader tokenization growth**, with the tokenized real-world asset (RWA) market surpassing $24B in on-chain value in 2025[14] and projections of $16T in RWA tokenization by 2030[15] as banks and asset managers continue to tokenize additional securities
- **Opportunities as a tokenized cash solution** to operate on expanding ledger-based payments infrastructure[16]
- **Improving regulatory and operational readiness** strengthening the infrastructure and business case for deposit tokens, with global regulatory developments for tokenization, blockchain, and digital assets, enabling banks to adopt these solutions.

DEPOSIT TOKEN CHALLENGES

- Despite strong growth, many deployments remain pilots except for a handful in full production, which may slow down scale. The market for deposit tokens has yet to mature and is primarily institutional.
- Relatively small size of overall deposit-token issuance compared to the broader financial system, indicating that large-scale adoption is still emerging.
- Scalability depends on addressing existing regulatory, operational, liquidity, interoperability and risk-management challenges
- While data often refers more broadly to tokenized deposits, which include deposit tokens, separating deposit tokens from larger tokenization trends and stablecoins can be difficult.

II) ECOSYSTEM VIEW OF DIGITAL MONEY

This section provides an ecosystem view of key stakeholders and their interactions. We start with an ecosystem table below, specifying the entities involved and their respective roles:

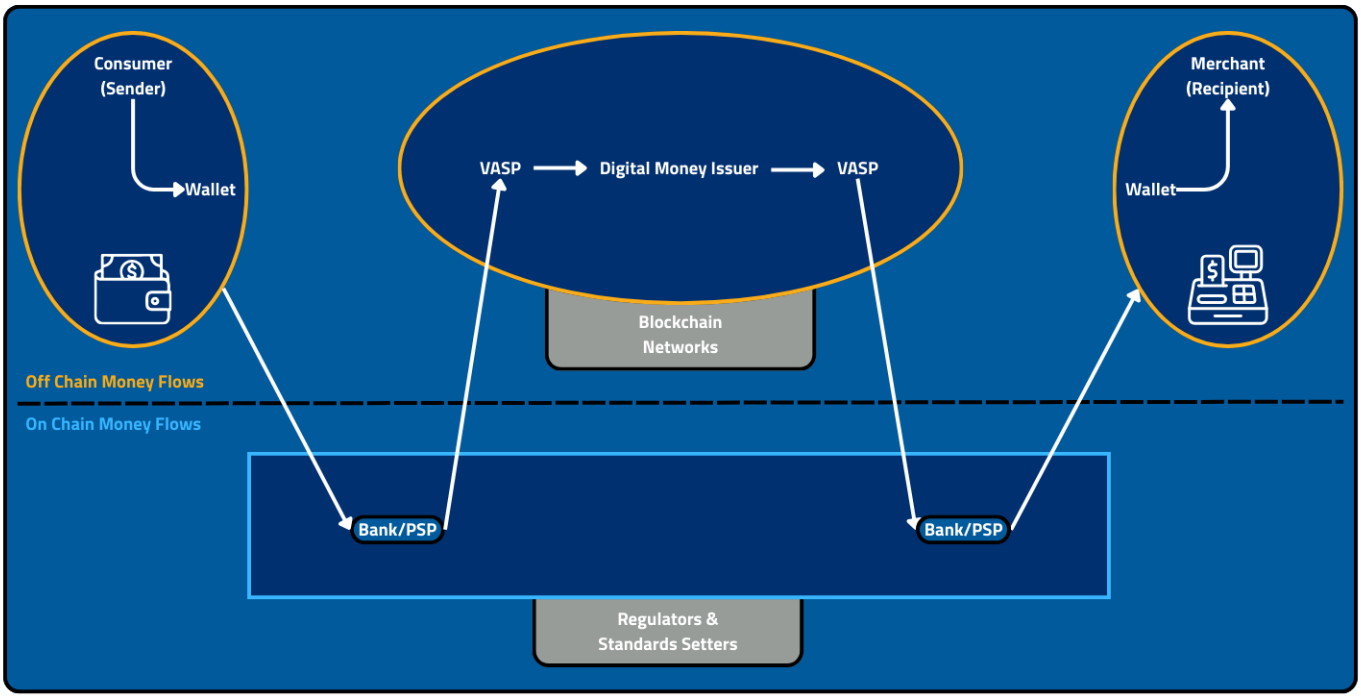
Key Stakeholders in Digital Money Ecosystem

Examples	Jurisdiction
Issuers of Digital Money	Create the digital asset/token used for payments
Wallets & Account Providers	• Enable users to hold digital money and make transactions • Wallets act as the interface into the blockchain space, with functions like key management • Wallets represent/act on behalf of users in the blockchain space
Banks & Payment Service Providers (PSPs)	Facilitate value transfers across entities and individuals
Blockchain Networks	Infrastructure to record and verify transactions
Virtual Asset Service Provides (VASPs)	On/Off Ramps, providing a bridge between traditional finance and digital assets
Merchants/users (end pt)	Accept payments with digital assets
Consumers/users (starting pt)	Make payments using digital assets
Regulatory Oversight/Authorities & Standards Setting Bodies	Ensure compliance with regulatory requirements, standards, and risk management practices

Although traditional and ledger-based scenarios may have a different set of key stakeholders, they share a common objective when it comes to payments functionality. While different infrastructure and different sets of stakeholders between ledger-based and traditional payment systems may define separate starting points with respect to operations, the common end goal of facilitating payments brings convergence.

Below is a generic use case of blockchain-based digital money for payments, illustrating the interactions between the key stakeholders. The digital money flows and key stakeholder interactions would be similar for all payments use cases of blockchain-based digital money, including e-commerce, in-store POS, B2B payments, and peer-to-peer (P2P) transfers – all payment flow models that can also be carried out with traditional systems.

Generic Model of Stakeholder Interactions using blockchain-based digital money

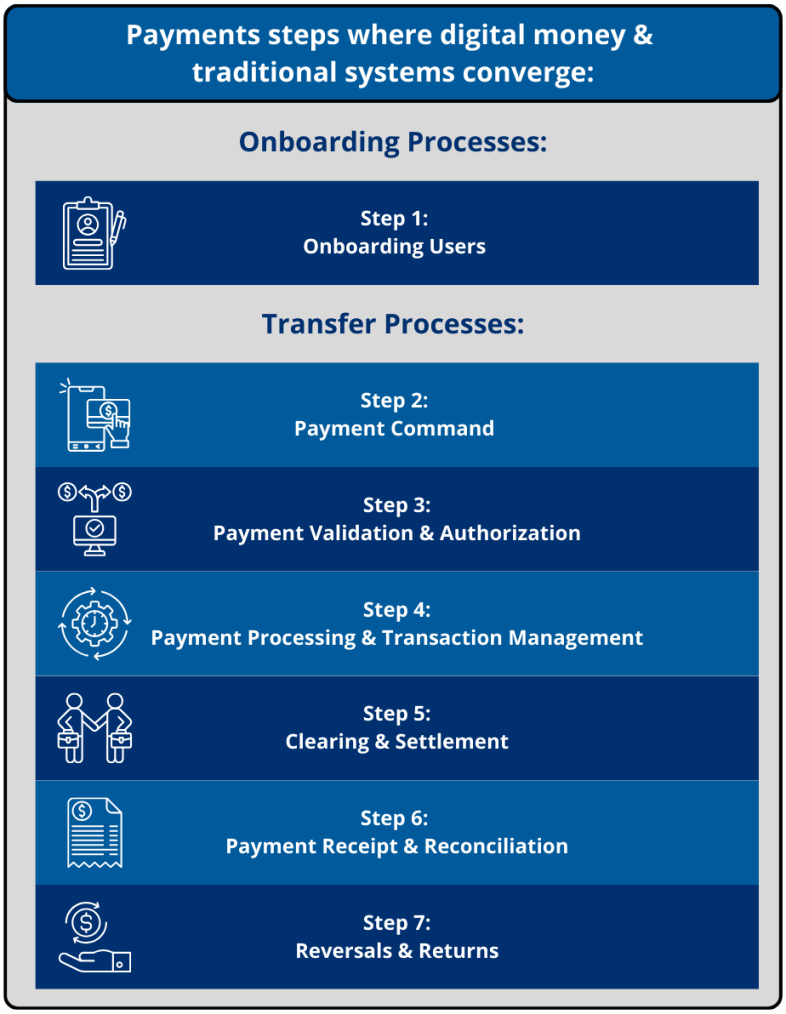


Ultimately, the activities performed to ensure a successful payment transaction, although carried out by different parties in the traditional and ledger-based scenarios, are similar in nature. Thus, the stakeholders involved in the blockchain-based digital money ecosystem take on similar roles as those in traditional payment arrangements. This becomes especially clear as regulations and risk management frameworks are put into place. With the broader regulatory approach of same activity - same risk - same regulation, we begin to observe the two worlds of traditional and ledger-based systems coming together.

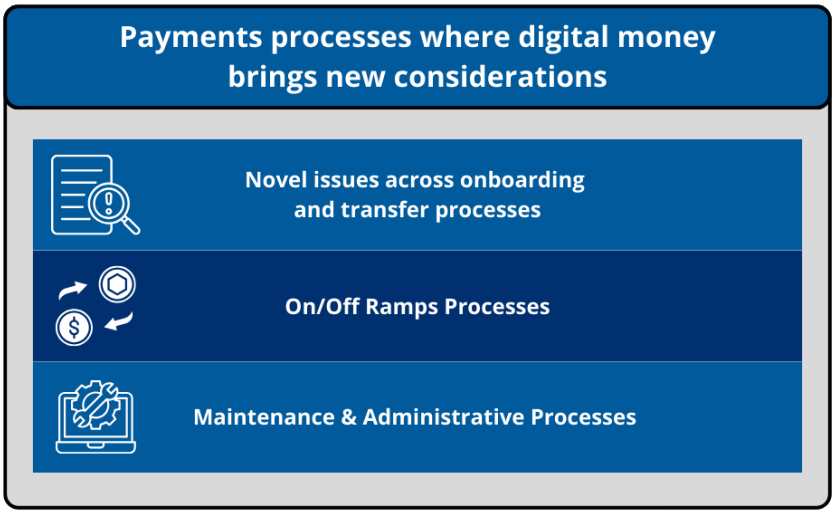
III) VALUE CHAIN OF PAYMENTS WITH DIGITAL MONEY

This section assesses the end-to-end flow of the payments process, from the steps required to complete a payment operation, to the processes involved. We evaluate the processes involved in the payments value chain using blockchain-based digital money. While many of these steps converge with traditional payment systems, there also arise novel issues. All these processes are subject to a series of regulatory requirements and standards – both for traditional payments and also blockchain-specific standards.

Convergence between traditional & digital money: As stated, prior, when regulatory requirements and risk mitigation frameworks are put into place, the payments process for blockchain-based digital money converges with traditional models. We find that many steps involved along the payments process for blockchain based digital money mirror the steps involved for traditional payments.



Novel Processes arising from blockchain-based digital money: Nevertheless, blockchain based digital money stills add certain novel issues for payment processes



Importance of Standards

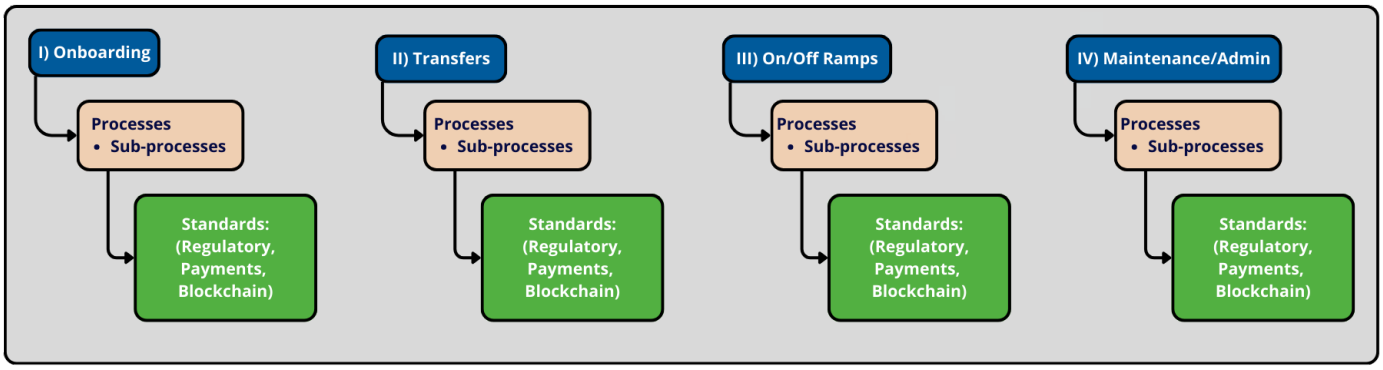
An end-to-end blueprint for payments – where each process is mapped out against relevant regulatory requirements and standards – is meant to help design a payment system architecture that is compliant with global standards for payments and data. A well-defined blueprint that identifies standardized requirements across every step of the payments value chain is meant as a useful tool to ensure interoperability, security, and scale, ultimately supporting the various payments use cases. With this intent, for each stage of the payments lifecycle, we highlight relevant standardized requirements that may take the form of regulatory requirements, payments standards and messaging protocols, and blockchain standardization efforts. This mapping can be a useful tool guiding how to build a system - specifically what standards to adhere to and best practices to ensure viability.

We note that for blockchain and digital assets, there have been substantial efforts toward standardization – a field that is mapped out in the Technical Standards GSMI report and Landscape. We highlight those standardization efforts that are relevant for payments, ranging from standards produced by globally recognized bodies which have gone through formal approval processes (e.g., ISO, IEEE, ITU-T), to industry-led standardization initiatives that have gained widespread adoption in the absence of more formal standards (e.g., ERC). Many of these are standardization approaches are for structuring payment tokens and their use, in addition to interoperability. For instance, existing token standards, which are crucial for settlement, must be shared between parties to ensure fund flows.

II.I) PROCESSES FOR DIGITAL MONEY PAYMENTS & STANDARDS

Below is a detailed end-to-end flow of specific processes involved in digital payments processing with blockchain-based digital money and the relevant frameworks (regulations and standards) for each step. The process map below categorizes payment processes according to the nature of payment activity (onboarding, transfers, on/off ramps, and maintenance/admin), and the identifies relevant existing standards. We note that processes may occur simultaneously, or get split up across the different steps of the payments lifecycle illustrated above. Rules may apply to the entire lifecycle or apply to certain stages or jurisdictions.

Processes Landscape*



**Note: Standards are listed below each overall process. Any exceptions or additions relevant to a specific process/sub-process are placed below that process/sub-process*

I) ONBOARDING: Registering users onto a payments platform

1.1) Onboarding Processes

1.1.1) KYC

- Identity Verification & Digital Identity
- Government ID & verification
- Biometric ID verification (e.g., you are who you say you are)
- Users provide basic data (e.g., address, email, phone number)

1.1.2) Account opening/Wallet creation

- Associate name in acct (connected to email/phone/govt ID, connected to key generated for acct) to info from KYC
- Verification levels as annotation to acct, allow user to do diff volumes of transactions based on KYC level

1.1.3) Key Generation (to enable transactions)

- Whitelisting after key is generated (allowing address to transact vs not)
- Providing digital identity to users

1.1.4) AML/CFT

- Source of funds verification
- Transaction Monitoring
- Screening & Reporting

1.2) Onboarding Standards

1.2.1) Legal & Regulatory

- EU Payment Services Directive (PSD2) - European open banking requirements[17]
- European Banking Authority (EBA) Guidelines - Various guidelines for several aspects of payment services, to enhance security, competition, and consumer protection[18]
- European Digital Identity Framework - framework for universal, trustworthy, and secure European digital identity, enabling creation of a digital identity wallet[19]
- EU Fifth Anti-Money Laundering Directive (AMLD5)[20] - AML/CFT regulations, addressing risks associated with virtual currencies
- FATF Recommendations[21]: AML and CFT procedures, including customer due diligence (CDD), with provisions for virtual currencies
- EU eIDAS (EU): Electronic identification and trust services; defines assurance levels for onboarding in the EU
- EBSI DID/Verifiable Credentials Framework - framework for expressing, exchanging, and verifying information
- Additional legal/regulatory requirements may depend on licensing requirements

1.2.2) Payment Standards

- ISO/IEC 29003: Guidelines for digital identity proofing, authentication, and validation.
- ISO 20022 - Standard for electronic data exchange between financial institutions. Includes standardized data structures for legal entity identifiers (LEIs)
- ISO 17442 (GLEIF) - Global Legal Entity Identifier (LEI) System to identify participants in financial transactions
- ISO 17442-3 (GLEIF) - verifiable Legal Entity Identifier (vLEI) for a digitally signed, tamper-resistant credential for decentralized authentication of legal entities
- ISO/IEC 29115 - Standard framework for managing entity authentication assurance
- NIST SP 800-63-3 (US): Digital Identity Guidelines NIST Levels of Assurance (LOA) - IAL1–3, AAL1–3 - Guidelines for digital onboarding

1.2.3) Blockchain Standards

- RMF: Risk Mitigation Framework (RMF)[22] – for non-financial risks of blockchain infrastructures
- IEEE standards on interoperability and payments
- IEEE 3205-2023 - IEEE Standard for Blockchain Interoperability Data Authentication and Communication Protocol
- P3205/D5.0, Aug 2022 - IEEE Draft Standard for Blockchain Interoperability - Data Authentication and Communication Protocol
- P2143.3 - Standard for Risk Control Requirements for Cryptocurrency Payment (Under Development)
- P2048.202 - Standard for Security Specifications of Blockchain-Based Metaverse Data (key for payment security in metaverse)
- ITU-T: Study Group 17 (Security): Addresses DLT security, threats, frameworks, and guidelines for digital identity and payments. Standards include definitions (X.1400), security threats (X.1401), and security for digital payment services (X.1405).
- IETF: Network & Data Transport Layers[23] - RFC 8578 (DetNet Use Cases), including point-to-multipoint and low-latency transport suitable for blockchain traffic in deterministic networks

II) TRANSFERS: Sending funds across registered users

2.1) Transfer Processes

2.1.1) Payment Command

- Payment Instruction & Initiation
- Data Exchange
    - Blockchain Standards for Data Exchange
        - **IVMS101:** InterVASP Messaging standard providing common language for communication of required originator and beneficiary information between VASPs, focused on Travel Rule compliance.[24]
        - **TRUST (IEEE 2418.2-2020):** data format requirements for blockchain systems.[25]
        - **Notabene/Transaction Authorization Protocol (TAP):** Built on TAP, Notabene provides an open, interoperable messaging layer for pre-transaction authorization and compliance. TAP uses IVMS101.[26]
        - **ITU-T: Study Group 17 (Security):** Addresses DLT security, threats, frameworks, and guidelines for digital identity and payments. Standards include definitions (X.1400), security threats (X.1401), and
- AML/CFT (triggered after user initiates transfer)
    - Blockchain Standards for AML/CFT
        - **Notabene/Transaction Authorization Protocol (TAP):** Built on TAP, Notabene provides an open, interoperable messaging layer for pre-transaction authorization and compliance. TAP uses IVMS101.[27]
        - **ITU-T: Study Group 17 (Security):** Addresses DLT security, threats, frameworks, and guidelines for digital identity and payments. Standards include definitions (X.1400), security threats (X.1401), and security for digital payment services (X.1405).

2.1.2) Payment Validation & Authorization

- Payment Approval
- Payment Standards may not be relevant for Payment Validation & Authorization, as internal processes focus on regulatory compliance

2.1.3) Payment Processing & Transaction Management

- Internal operations by an entity or network for payment to go out
- Payment qualification
- Deposits & Withdrawals: Movement of funds between bank accounts and blockchain addresses (typically performed internally by a single entity)
- Sending of funds
- Receipt of funds
- Delegated transfers: authorized by 3rd parties including other smart contracts
- Alias-based transfers: Use easy to remember identifiers instead of wallet addresses
- Legal & Regulatory Requirements for Payment Processing & Transaction Management
    - Jurisdiction-specific stablecoin regulations - Jurisdiction-specific
    - Jurisdiction-specific taxation requirements, including capital gains taxes
- Payment Standards may not be relevant for Payment Processing & Transaction Management, as internal processes focus on regulatory compliance

2.1.4) Clearing & Settlement

- Atomic transactions
- Legal & Regulatory Requirements for Clearing & Settlement
    - **EU Settlement Finality Directive (SFD) –** designed to avoid systemic risk, ensuring transfer orders within systems become legally final and enforceable, even if a participant becomes insolvent
- Payment Standards for Clearing & Settlement
    - **ISO 20022 -** Standard for electronic data exchange between financial institutions. PACS.008 - ISO 20022 message for financial institution to financial institution customer credit transfers, crucial for cross-border payments
    - **SWIFT MT 103 -** customer payment message to transfer funds from one bank account to another
    - **SWIFT MT 202 -** bank-to-bank transfer message to transfer funds between financial institutions
    - **US NACHA File Format (ACH) -** standardized file format used for Automated Clearing House (ACH) transactions
    - **Single European Payments Area (SEPA) Clearing and Settlement Mechanisms (CSMs) -** payments are processed by CSMs as intermediaries between Payment Service Providers (PSPs), with settlement occurring between PSP accounts at the European Central Bank (ECB)
- Blockchain Standards for Clearing & Settlement
    - Existing token standards' (e.g, TTF, ERC-20 included in Transfers – Blockchain Standards list below) provisions for settlement require sharing data between parties

2.1.5) Payment Receipt & Reconciliation

- Deposit of funds into recipient wallet
- Confirmation of receipt of funds
- Legal & Regulatory Requirements for Payment Receipt & Reconciliation
    - Reconciliation of omnibus allocation - required for certain entities depending on the jurisdiction
    - AML regulations (included in Transfers- Legal & Regulatory Requirements list below) may require reporting source of funds, specifying those with greater AML risks

2.1.6) Reversals & Returns

- Identify principal custody
- Initiate new transaction to return funds - decision making and approval structures for "reversing" a validated transaction (e.g., usually request funds to recipient wallet, but in extreme cases a fork)
- Payment network rules and merchant policies may determine internal procedures
- Legal & Regulatory Requirements for Reversals & Returns
    - Requirements for Automated Clearing House (ACH) transactions including timeframes, reason codes to process returns, and formatting
    - Jurisdiction-specific consumer protection regulations for unauthorized transactions (e.g., UK Payment Services Regulations) and accurate reporting (e.g., US Fair Credit Reporting Act (FCRA))

- Payment Standards for Reversals & Returns
    - **ISO 20022 -** Standard for electronic data exchange between financial institutions. Includes standardized data structures for legal entity identifiers (LEIs)
    - S**WIFT MT & MX -** SWIFT messages, considering MX messages, built on ISO 20022, offer more structured and richer data that reduces ambiguity and facilitates greater automation for reconciliation
    - **National Automated Clearing House Association (NACHA) operating rules and return codes -** rules govern ACH Network, including return codes indicating why an ACH transaction may have been unsuccessful

2.2) Transfer Standards

2.2.1) Legal & Regulatory

- **FATF Travel Rule -** Requires sharing information about fund transfers, senders, and recipients, including those involving crypto assets
- **EU Wire Transfer Regulation (WTR) –** For EU compliance with the Travel Rule
- **EU Payment Services Directive (PSD2)[28] -** European open banking requirements
- **European Banking Authority (EBA) Guidelines[29] -** Various guidelines for several aspects of payment services, to enhance security, competition, and consumer protection.
- Additional legal/regulatory requirements may depend on licensing requirements

2.2.2) Payment Standards

- **ISO 20022 -** Standard for electronic data exchange between financial institutions. Includes standardized data structures for legal entity identifiers (LEIs)
- **SWIFT MT 101 & MX -** SWIFT message type to request transfers of funds, considering MX messages are built on ISO 20022, which offers more structured and richer data that reduces ambiguity and facilitates greater automation for reconciliation, such that ISO 20022 compliance most likely leads to SWIFT compliance by default
- **Single European Payments Area (SEPA) Credit Transfer (SCT) -** electronic funds transfers between bank accounts within the SEPA region
- **Single European Payments Area (SEPA) TARGET Instant Payment Settlement (TIPS) -** Extension for instant retail payments

2.2.3) Blockchain Standards

- IEEE standards on interoperability and payments
    - **IEEE 3205-2023 -** IEEE Standard for Blockchain Interoperability Data Authentication and Communication Protocol
    - **P3205/D5.0, Aug 2022 -** IEEE Draft Standard for Blockchain Interoperability - Data Authentication and Communication Protocol
    - **2143.1-2020 -** IEEE Standard for General Process of Cryptocurrency Payment
    - **P2143.2 -** Standard for Cryptocurrency Payment Performance Metrics (Under Development)
    - **P2143.3 -** Standard for Risk Control Requirements for Cryptocurrency Payment (Under Development)
    - **P3272.01 -** IEEE Standard for Blockchain Based Stablecoins Payment Service

Requirements
    - Survey on Blockchain-based IoT Payment and Marketplaces
    - **P2048.202 -** Standard for Security Specifications of Blockchain-Based Metaverse Data (key for payment security in metaverse)
    - **IEEE P2145 -** Standard for Framework and Definitions for Blockchain Governance
- IETF
    - **Network & Data Transport Layers[30] -** RFC 8578 (DetNet Use Cases), including point-to-multipoint and low-latency transport suitable for blockchain traffic in deterministic networks
- **Secure Asset Transfer Protocol (SATP) & Interoperability Drafts[31] -** intended to standardize secure movement of digital assets across blockchain networks through API gateway architectures
- **Token Taxonomy Framework (TTF) -** for token design and issuance, designed to improve interoperability
- **ERC Standards -** focus largely on token standards and functionality
    - *ERC-20* – standard set of functions for fungible tokens, transfers, and delegated transfers. Relevant for account-based ledgers and setting a foundation for other standards
    - *ERC-721* – NFTs
    - *ERC-777* – Enhanced functionality over ERC-20
    - *ERC-1155* – Multi-token standard, supporting single and batch transfers, introducing operator approvals for delegated transfers
    - *ERC-1400* – Security tokens, and tokenizing traditional financial assets, allowing delegated transfers with compliance checks
    - *ERC-3643* – Permissioned token standard focused on compliance & transfer, relevant for security tokens. Enhanced version of ERC-20 model with additional compliance verifications. Supports on-chain identities.
    - *ERC-865 (proposed)* – Simplifying token transfers through fees embedded in the transferred token itself to reduce frictions
    - *ERC-4337* – facilitates delegated transfers and account-abstraction functionalities
- **Interledger Protocol -** Interoperability for cross-ledger payments
- **Risk Mitigation Framework (RMF)[32] –** for non-financial risks of blockchain infrastructures

III) ON/OFF RAMPS: Converting funds between fiat and blockchain-based digital money

3.1) On/Off Ramp Processes

1. **Fiat side: Reserve management**
2. **Blockchain side: Issuance & destruction of tokens**
    - Minting tokens
    - Burning tokens
3. **Reconciliation of blockchain side against fiat side**
    - Reconcile mint/burn against on chain tokens

3.2) On/Off Ramp Standards

3.2.1) Legal & Regulatory

- Regulatory requirements under development, as this is an emerging space

3.2.2) Payment Standards

Payment standards under development, as this is an emerging space

3.2.3) Blockchain Standards

- Token standards
    - Token Taxonomy Framework (TTF): for token design and issuance, designed to improve interoperability
    - ERC-20
- Risk Mitigation Framework (RMF)[33] – for non-financial risks of blockchain infrastructures
- IEEE standards on interoperability and payments
    - IEEE 3205-2023 - IEEE Standard for Blockchain Interoperability Data Authentication and Communication Protocol
    - P3205/D5.0, Aug 2022 - IEEE Draft Standard for Blockchain Interoperability - Data Authentication and Communication Protocol
    - P2048.202 - Standard for Security Specifications of Blockchain-Based Metaverse Data (key for payment security in metaverse)
    - IEEE P2145 - Standard for Framework and Definitions for Blockchain Governance

IV) MAINTENANCE/ADMIN: Support processes to ensure adequate functions throughout, including governance, administrative controls, and privileged functions

4.1) Maintenance/Admin Processes

4.1.1) Accounting Ledger

- View activities from processes above
- Track and update records of balances
- **Blockchain Standards for Accounting Ledger**
    - *ERC-20 (for account based)*
    - *ERC-721: (for fixed denomination)*
    - *E-cash for fixed denomination tokens*

4.1.2) Remuneration

- Calculation, accrual, and crediting of returns
- DeFi functionalities to calculate interest may apply

4.1.3) Deposits & Withdrawals

- Allow movement of funds between accounts and blockchain addresses

4.1.4) Permissioning

- Manage permission levels for administrative access
- Allow permissioned transfers, with underlying rules to approve or deny token transfers
- **Blockchain Standards for Permissioning**
    - *ERC-1400: transfer restrictions and regulatory compliance for permissioned transfers*
    - *ERC-3643: On chain ID verifications and whitelist controls*
    - *ERC-6997: Adds transaction validation step to ERC-721*

4.1.5) Payment Information: Collection & Communication

- **Blockchain Standards for Payment Information**
    - *ERC-735: allows third parties to issue claims about a specific identity*
    - *ERC-3643: enables off chain rule specification on an on chain registry*

4.1.6) Federated Access Control: Trusted entities can enforce policies for token access

- **Blockchain Standards for Federated Access Control**
    - *ERC-1400: Access control can be part of compliance framework*
    - *ERC-3643: Allows multiple trusted entities to manage and enforce policies for access over token transfers*
    - *ERC-6617: Bit-based permissioning scheme*
    - *EIP-7820: Allows standardized access control registry*

4.1.7) Key Rotation & Account Recovery: Allow users to update keys or recover accounts in cases of lost keys

- **Blockchain Standards for Key Rotation & Account Recovery**
    - *ERC-1400: Partial key recovery support*
    - *ERC-3643: Enables key recovery and rotation mechanisms for regulated assets, integrated with on-chain identity*

4.1.8) Enabling/disabling of accounts

- Freezing tokens and seizing tokens under specified conditions

4.1.9) Pausing Transactions

- **Blockchain Standards for Pausing Transactions**
    - *ERC-3643: Includes functions to pause/suspend transactions in case of emergency*
    - *OpenZeppelin Pausable Function: Smart contract module allowing a smart contract to halt critical functions temporarily*

4.1.10) Smart contract upgrades

- Upgrading token logic
- **Blockchain Standards for Smart Contract Updates**
    - *ERC-1882: Upgrade path with minimal and efficient means*
    - *ERC-2535: Diamond Standards, specifically engineered for modular upgrades*
    - *ERC-3643: Allows updates to contract logic without disrupting token balances*

4.1.11) Gasless Transactions

- Allowing third parties to cover gas fees on behalf of users
- **Blockchain Standards for Gasless Transactions**
    - *ERC-3009: Allows third parties to submit authorized transactions and pay gas fees*
    - *ERC-4337: decentralized entities can sponsor gas fees for bundled transaction object*

4.2) Maintenance/Admin Standards

4.2.1) Legal & Regulatory

- Regulatory requirements under development, as this is an emerging space

4.2.2) Payment Standards

- Payment standards under development, as this is an emerging space

4.2.3) Blockchain Standards

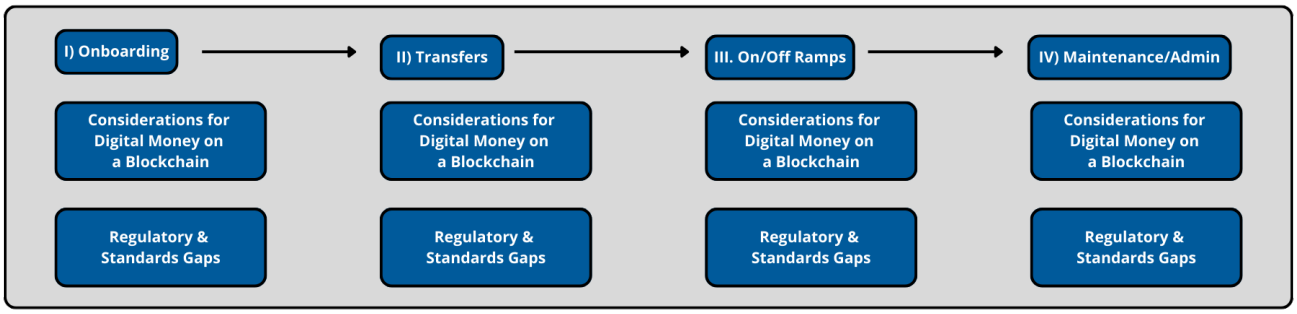
- Token standards
    - *Token Taxonomy Framework (TTF) - for token design and issuance, designed to improve interoperability*
    - *ERC-20*
- Risk Mitigation Framework (RMF)[34] – for non-financial risks of blockchain infrastructures
- IEEE standards on interoperability and payments
    - *IEEE 3205-2023 - IEEE Standard for Blockchain Interoperability Data Authentication and Communication Protocol*
    - *P3205/D5.0, Aug 2022 - IEEE Draft Standard for Blockchain Interoperability - Data Authentication and Communication Protocol*
    - *IEEE P2145 - Standard for Framework and Definitions for Blockchain Governance*
    - *P2048.202 - Standard for Security Specifications of Blockchain-Based Metaverse Data (key for payment security in metaverse)*
    - *IEEE P2145 - Standard for Framework and Definitions for Blockchain Governance*

III.II) DEEP DIVE INTO NEW CONSIDERATIONS

Digital money introduces novel issues across each stage of the payments lifecycle. In assessing the payments lifecycle for digital money, we identify these new considerations for blockchain-based digital money and existing gaps in regulations and standards. With a wide variety of different senders and recipients, alongside different standards that may apply to apply to various stages of the payments lifecycle, we identify areas where there may be no clear standards for payments with digital money.

These are issues where the industry needs to come together beyond the existing standards to agree on harmonized rules for payments. While many of these novel issues, especially where there may be gaps in regulatory requirements and global standards, are already being addressed by the industry, there is still a need for greater harmonization.

New Considerations for Digital Money and Existing Regulatory & Standards Gaps



I) ONBOARDING

- Considerations for Blockchain Based Digital Money
  - AML/CFT may be carried out differently in the context of tracing flows of funds on a blockchain. There may be use of a plugin (e.g., Chainalysis/Elllyptic), which requires ensuring the plugin works and integrations with the right wallets, senders/recipients, and any other relevant entities.
  - For AML, depending on backside of any bank connections, there may be a principal bank omnibus account or 3rd party banks that can make deposits or withdrawals
  - KYC for onboarding may be conducted in various forms, requiring use of an SDK or other internal processes
  - Digital identity is fundamental for decentralized transactions to take place - both for individuals/entities; and for funds, whether they be digitally native or representations of fiat funds on a blockchain

- Regulatory & Standards Gaps
  - Identity standards, which consist in proving the identity of individual sand entities, may fall largely outside the scope of payments. There are several digital identity standards globally and various national identity models (e.g., Aadhaar - API based electronic KYC framework for biometric-based ID verification), some of which may provide KYC frameworks for secure identity verification
  - AML/CFT/KYC & DID - mostly set requirements for traditional rails
  - Gaps around wallet initialization requirements
  - Gaps around custody requirements

II) TRANSFERS

- Considerations for Blockchain Based Digital Money
    - US Fed's FedNow Integration with ISO[35]: FedNow instant payment service (launched in July 2023) uses the ISO 20022 messaging standard. Standardization facilitates interoperability between payment systems and supports integration for blockchain-based payment solutions.
- Regulatory & Standards Gaps
    - ISO is highly rigorous and specialized, in ways that may not translate to transactions with tokens. ISO is meant to be broad, capturing varied scenarios, but the nested structure becomes complex and challenging to apply to blockchain-based digital money models.
    - SWIFT messaging standards (MT standards and updated MX standards) are aligned to ISO 20022, such that compliance with ISO also implies compliance with SWIFT. The same challenges to apply to digital money tokens apply.
    - European open banking messaging standards are also envisioned for traditional banking models, requiring nuance for application to blockchain-based digital money
    - Regulatory requirements are yet to be harmonized
    - Adherence to standards that may remain as blockchain industry initiatives
    - Absence of risk reporting requirements
- **Additional considerations specific to processes for payment transfers below**

2.1) Payment Command

- Considerations for Blockchain Based Digital Money
    - Peer to peer vs. intermediation
    - Additional legal/regulatory requirements may depend on licensing requirements

2.2) Data Exchange

- Considerations for Blockchain Based Digital Money
    - Format in which to exchange data
    - Privacy considerations and best practices (e.g., not sharing PII on chain)
    - Separate avenues to share confidential data vs what can be shared on chain
    - Data flows determine the ability to perform authorizations for payment operations using digital money. First, it is fundamental to identify what players are communicating with each other, understanding the business logic of any payments process using digital money. Second, it is necessary to identify how these players are communicating (e.g., over APIs, on a blockchain), and if existing standards are applicable for these communications (e.g., API connectivity structured according to ISO 20022).
    - For instance, VASPs need data (e.g., sufficient funds checks, economic activity correlations) to apply controls they are obliged to perform. Exchanging data and communicating with other VASPs can increase frictions, due to the need for separate off-chain networks to exchange confidential information.

        - Some VASPs have addressed this issue by developing trust networks that simplify the required exchange of data.
        - Reporting is contingent upon VASP internal risk analyses. This can raise concerns in light of the Travel Rule under FATF recommendations, which requires senders and recipients to share data. Payment information must always go from the sender to recipient financial institution. Yet certain jurisdictions may have a threshold under which these rules may not apply. Therefore, there can be cases where senders may not release tokens to recipients when the required data is not available, and other cases where there fund transfers may take place with no need for the data sharing (e.g., raising concerns for EU customers where Travel Rule requirements are clearly specified).
- Standards Gaps
    - Standards for many blockchain-based privacy preserving tools may remain as industry initiatives, prior to recognition by globally recognized standards setters

2.3) AML/CFT

- Considerations for Blockchain Based Digital Money
    - Format to share data and privacy considerations

2.4) Payment Validation & Authorization

- Considerations for Blockchain Based Digital Money
    - Payment approval may not be carried out by a centralized party and may be automated with a smart contract based on pre-set conditions
    - Travel Rule considerations in the context of exchanges, decentralized infrastructure
    - Jurisdiction specific requirements may vary
    - The greatest focus at this stage is to adhere to regulatory requirements, highlighting the importance of internal processing to remain compliant. Standards other than regulation become less relevant.

2.5) Payment Processing

- Considerations for Blockchain Based Digital Money
    - Smart contract considerations for automated payments (e.g., conditions for payer to have funds and recipient to have an adequate wallet to receive them)
    - Considerations for fund transfers between centralized and decentralized systems
- Standards Gaps
    - Payment processing involves multiple internal processes, where regulatory requirements for risk mitigation may precede technical standards. Payment routing to determine the optimal path for funds to travel from payer to recipient may no longer be relevant for digital money over p2p and disintermediated transfers.

        - There are no harmonized requirements to address smart contract vulnerabilities
        - Authorized forms of digital money to carry out transactions may be unclear (e.g., in Japan it's illegal to use stablecoins that are not authorized (e.g., USDT), but there are no sanctions if people do use these stablecoins)

2.6) Clearing & Settlement

- Considerations for Blockchain Based Digital Money
    - Digital money operates outside the traditional 2-tiered model of money, where clients of different banks can settle on central bank money. For digital money, atomic settlement combines both clearing and settlement into a single operation. There is no central bank behind transacting parties to enable fungibility between different forms of money, which highlights the importance of interoperability (e.g., exchanging between stablecoins and CBDCs).
- Standards Gaps
    - In the traditional banking model, central banks provide a public good by enabling fungibility across parties to exchange currencies. Local fiat money exchanges are generally standardized across local payment networks.
    - For digital assets, FX considerations among different currencies are an area in need of standardization. For instance, liquidity pools may use external exchange rates, while other parties may use internal exchange rates. Exchanging between currencies may result in spreads and earnings. Certain payment solutions may have plugins to omnibus accounts with access to several forms of digital money, including fiat-based models that operate on SWIFT and ACH networks.
    - This becomes an issue with economic implications.

2.7) Payment Receipt & Reconciliation

- Considerations for Blockchain Based Digital Money
    - While traditional models involve internal bank processes to carry out reconciliations in compliance with standards (e.g., linking payment receipts with bank entries, requirements for automating reconciliations), digital money introduces novel issues for depositing funds directly into recipient wallets.
    - Architecture of payment infrastructure impacts reconciliation of user funds (e.g., using omnibus on/off ramp accounts vs. sending funds directly to individual wallets).
- Standards Gaps
    - For digital money using blockchain, it has become a best practice to utilize forensics tools designed for blockchain fund transfers, to track and trace funds, which allow filtering & analyzing the source of funds
    - For funds sent directly to user wallets, there is an expectation for them to pass AML requirements, but they may not need to reconcile with omnibus accounts and subaccounts.
    - For funds sent to wallets/exchanges that utilize omnibus accounts, there's an expectation for omnibus account allocations to credit users' individual wallets

- In the absence of risk reporting requirements, certain players have developed a wallet network-based approach to segregate funds by risk, where funds that trigger higher risks are sent to certain designated wallets, or in an omnibus structure, to sub wallets categorized by AML that are segregated from both main omnibus funds and users.

2.8) Reversals & Returns

- Considerations for Blockchain Based Digital Money
  - From a rulebook perspective, VASPs can be treated as intermediaries in traditional payments systems
  - From a technical perspective, reversing a payment would not cancel the original payment but add a new payment
  - From a legal perspective, if funds were sent to the wrong address (either by mistake or maliciously), there are usually structures to compel the recipient to return the funds (e.g., suing if needed), along with operational processes to perform the reversal. In a decentralized structure, however, it may be unclear whom to target (e.g., the network deciding to unwind funds, the recipient, the wallet, etc.)
  - Transactions between self-hosted wallets, however, add complex challenges and uncertainties. When users maintain their own wallet, hosted within a multi-party computation system (MPC) in a co-hosting application, the wallet's host maintains the ability to send funds back to the source (e.g., AML reasons or other motives). This brings considerations regarding governance structures
  - Considerations around self-hosted, custodial wallets
  - Governance structures and clawback features to make unwinding a possibility
- Standards Gaps
  - Need for agreement to develop standards - by token, by VASP, etc.
  - While ERC-20 has no reference code, transaction codes may be a possibility for on-chain settlement

III) ON & OFF-RAMPS

- Considerations for Blockchain Based Digital Money
  - Compliance with regulations & standards (payments & blockchain)
- Standards Gaps
  - Globally recognized standards and regulatory frameworks are still in development

IV) MAINTENANCE/ADMIN

- Considerations for Blockchain Based Digital Money
    - Decentralized governance
    - Most processes are specific to blockchain infrastructure
- Standards Gaps
    - Accounting Ledger: No standards to record UTXO form on EVM
    - Remuneration: No standard or widely adopted practice
    - Collection & communication of payment information with banks: No standard exists for this feature
    - No adequate standards for enabling/disabling accounts
    - Globally recognized standards and regulatory frameworks are still in development

III.III) ADDRESSING REGULATORY & STANDARDS GAPS

The gaps in existing frameworks must be addressed to respond to the novel issues introduced by blockchain based digital money. We expect that as standards and regulatory requirements continue to develop, existing gaps will be addressed, and the blockchain-based digital money payments space will continue to converge with the traditional payments structures and approaches.

We find that most of the regulations and payments standards are envisioned for traditional payments architectures. Regulations are under development for blockchain and digital assets, while existing payment standards have yet to incorporate blockchain infrastructure considerations. Even among blockchain-based standards, there are elements in the digital money payments process that may not be covered. For instance, there are no clear standards for digital assets when it comes to clearing & settlement. While certain token standards may be applicable for settlement, requiring information sharing between parties, their applicability requires nuance.

Addressing standards gaps is especially important for processes related to on/off ramps, and for maintenance/governance, which raise novel issues almost in their entirety. In the absence of regulations and payments standards, blockchain standards specific to many of payment processes have arisen and gained significant adoption to harmonize practices. This is a space where blockchain standards may drive the development of mandatory regulations and formal payment standards in the future.

IV) REGULATORY DEVELOPMENTS FOR DIGITAL MONEY

Below is a global mapping of major regulatory developments relevant for blockchain-based digital money models we cover across this report. While stablecoins and deposit tokens are mapped against regulatory developments from major jurisdictions that have released requirements for blockchain and digital assets, CBDCs are subject to regulatory framework in their respective issuing countries. Therefore, CBDCs are not the focus the major global jurisdictions in the same way as stablecoins and deposit tokens, especially as none of the selected major jurisdictions below has yet launched a CBDC solution in production.

In order for payments solutions using blockchain based digital money to be seamless at a global level, digital money should be fungible across jurisdictions. For instance, a stablecoin that falls under a certain regulatory regime in one jurisdiction should be treated in a similar way under a separate regulatory regime for its adoption in another jurisdiction. In many cases, regulatory requirements may be specific to a token, but more commonly they apply to the entities engaging activities with these tokens (e.g., designated as VASPs or CASPs depending on the jurisdiction) – in line with the common practice to regulate the activity over the technology. There exist certain gaps for the seamless interoperable fungibility to occur today, especially when it comes to digital money models that are not fiat-backed. These forms of digital money generally don't fall under stablecoin-specific rules. Moreover, whether requirements which would apply for CBDCs may or may not be aligned with the frameworks above is yet to be determined.

Generic landscape of regulatory requirements for digital money

Digital Asset	Issuer/ Type	United States	EU (MiCA)	UK	Singapore	Hong Kong	Japan
Stablecoin	Private company / fiat-backed	• Compliance with GENIUS Act required to offer to US users for federal issuers • State regulators (e.g., NYDFS) for state-chartered issuers • AML/KYC (OFAC)	Electronic Money Institution (EMT) authorization required to offer to EU users	FCA authorization expected for fiat-redeemable stablecoins under UK regime when live	MAS SCS issuer license required, else falls within the DPT regime	HKMA FRS stablecoin issuer license required to offer to HK retail users. Professional investors and institutions can access non-HK stablecoins under the SFCs virtual asset regime	Distribution allowed only via licensed intermediaries; issuance restricted to banks/trusts/ FTSPs
CBDC	Central Bank / retail CBDC	• Issued and regulated by the Central Bank of the country issuing the respective fiat currency. • AML/CFT/KYC requirements, which financial institutions involved with the CBDC must adhere to					
CBDC	Central Bank / wholesale CBDC	• Issued and regulated by the Central Bank of the country issuing the respective fiat currency. • AML/CFT/KYC requirements, which financial institutions involved with the CBDC must adhere to					

Digital Asset	Issuer/ Type	United States	EU (MiCA)	UK	Singapore	Hong Kong	Japan
Deposit Token	Banking Institution / Deposit Token	Falls under the existing regulatory framework for commercial banks, including bank-specific prudential regulations, deposit insurance requirements, AML/KYC requirements, and compliance and internal procedures. Oversight includes U.S. federal and state banking and securities regulators, the Federal Reserve, the Office of the Comptroller of the Currency (OCC), and the U.S. Treasury Department's Office of Foreign Assets Control (OFAC)	Issuing banking institution authorization required or partnership with authorized entity under MiCA to offer deposit token in the EU, alongside specific requirements (e.g., reserves, liquidity, transparency disclosures, consumer protections)	Oversight under either the Financial Conduct Authority (FCA) or a dual regime with the Bank of England (BoE), depending on whether it's deemed "non-systemic" or "systemic" respectively.	• Oversight under the Monetary Authority of Singapore (MAS), and regulated under existing banking laws (Banking Act). They are distinct from the stablecoin regulatory framework, which applies to non-bank issued single currency stablecoins • Deposit tokens may fall within the ambit of digital payment tokens under the Payment Services Act 2019 depending on how they are structured and used	• Deposit tokens are treated as bank liabilities, falling under existing banking regulation • The Hong Kong Monetary Authority (HKMA) is actively developing regulations for deposit tokens through Project Ensemble, under the pilot EnsembleTX	• Regulated under the Payment Services Act (PSA), which established a framework for electronic payment instruments and stablecoins • Deposit tokens are treated as a form of electronic payment instrument if they represent a claim against a licensed bank. The PSA ensures stringent rules around issuance, reserve management, and segregation of funds.

IV.I) RECENT REGULATORY TRENDS FOR STABLECOINS

US

In the US, regulatory requirements must meet federal requirements and any relevant state-specific requirements, out of which we highlight NYDFS rules as a state that has released substantial guidance. While the U.S. has been a relatively fragmented in its approach, 2025 has shown a massive leap forward. The passage of the Guiding and Establishing National Innovation for U.S. Stablecoins Act, or the GENIUS Act, is a monumental achievement. After years of legislative debate, this law finally provides a clear federal framework for payment stablecoins. It codifies what much of the industry has been advocating for: a requirement for 100% reserve backing in cash or cash equivalents, regular public attestations from a third-party auditor, and clear redemption rights. The US GENIUS Act introduces a licensing framework where only approved Permitted Payment Stablecoin Issuers (PPSIs) can issue U.S.-pegged stablecoins, and must fully back them with high-quality liquid assets (e.g., T-bills), segregate reserves, avoid rehypothecation, and undergo monthly attestations.

Critically, it gives both federal and state regulators a clear mandate to oversee these assets, removing the regulatory ambiguity that has stifled innovation for so long. The GENIUS Act signals that the U.S. is serious about maintaining its role as a leader in financial innovation, and it provides a clear path for compliant issuers like Ripple to operate with confidence.

EU

The EU's Markets in Crypto-Assets regulation, or MiCA, is a landmark piece of legislation. It's the most comprehensive framework in the world for digital assets, and in some ways it can be a model for other jurisdictions. MiCA's approach to stablecoins is particularly robust. It creates two distinct categories:

- Asset-Referenced Tokens (ARTs): Stablecoins backed by a basket of currencies or assets.
- E-Money Tokens (EMTs): Stablecoins pegged 1:1 to a single fiat currency, like the euro or dollar.

For both, MiCA mandates stringent requirements. Issuers must be authorized by a competent authority, maintain full reserves of high-quality liquid assets, and publish transparent whitepapers and regular audit reports. For "significant" stablecoins - those with a large market cap and transaction volume over defined thresholds - the rules become even stricter, with enhanced supervision from the European Banking Authority.

This is a game-changer. It provides a clear legal pathway for compliant issuers and a high degree of confidence for institutional and retail users.

UK

The United Kingdom is also moving quickly, with new legislation aiming to bring stablecoins into its existing payments and e-money regulations. The focus is on fiat-backed stablecoins used for payments, with a phased approach to bring other crypto assets into the fold later.

Singapore

The Monetary Authority of Singapore has also finalized its regulatory framework, introducing a new "MAS-regulated stablecoin" label for Single Currency Stablecoins pegged to the SGD and G10 currencies. Issuers must meet stringent reserve, capital, and disclosure requirements to use this label, providing a clear seal of approval for users.

Hong Kong

In Hong Kong, the Hong Kong Monetary Authority has created a sandbox for stablecoin issuers, which allows issuers to experiment in a controlled environment with regulatory oversight until licenses for Fiat Referenced Stablecoins (FRS) are issued.

Japan

In Japan, authorities have long held a forward-looking stance, recently amending their Payment Services Act to regulate stablecoins. Only licensed banks, trust companies, and fund transfer agents can issue them, and they are required to hold reserves and ensure par redemption.

UAE

UAE regulators have introduced frameworks that support both fiat-backed stablecoins and tokenized assets, with an eye toward interoperability.

IV.II) RECENT REGULATORY TRENDS FOR CBDCs

US

The United States has taken an approach favoring stablecoins as the preferred form of digital money, with implications on the use of the US Dollar as the most popular reserve currency. With respect to CBDCs, a 2025 executive order essentially banned them by prohibiting federal agencies from taking action to create or promote a US CBDC, due to concerns regarding financial stability, privacy, and government overreach. The stance reverses previous research efforts and remains in contrast with other jurisdictions' trends exploring CBDCs.

EU

The EU is expected to release a Digital Euro, favoring a CBDC model over stablecoins. Stablecoins may be perceived as a less approachable option for banks due to a high deposit percentage requirement under current regulations.

UK

The UK is cautiously proceeding into, with the government and the Bank of England (BoE) in exploratory phases to assess the potential to introduce a digital pound CBDC.

Singapore

Singapore has a progressive regulatory stance toward CBDCs, focusing on a wholesale CBDC model for interbank settlements, and stating no immediate need for a retail CBDC model. The Monetary Authority of Singapore (MAS) has been actively involved in tests involving wholesale CBDCs and tokenized assets, with collaborative initiatives across jurisdictions including Project Ubin[38] and Project Guardian[39].

Hong Kong

The Hong Kong Monetary Authority (HKMA) has an active and progressive stance toward CBDCs, having led research and pilot programs since 2017 toward the development of a retail and wholesale model of an e-HKD. This CBDC is part of Hong Kong's endeavors to position itself as a digital finance hub.

Japan

Japan has a highly cautious approach, with the Bank of Japan (BOJ) stating no immediate plans to issue a digital yen CBDC despite being actively involved in research and pilot programs that would prepare for a potential future issuance. The country's high cash usage is recognized as a factor in the decision to evaluate a CBDC with caution.

China

China is actively developing and promoting its digital yuan (e-CNY), state control over its digital currency while maintaining strict controls the use of over other digital assets including cryptocurrencies. The e-CNY is being used for extensive pilot programs across various sectors, ranging from retail payments to public services.

IV.III) RECENT REGULATORY TRENDS FOR DEPOSIT TOKENS

US

Deposit tokens fall under the existing regulatory framework for commercial banks, including bank-specific prudential regulations, deposit insurance requirements, AML/KYC requirements, and compliance and internal procedures. Oversight includes U.S. federal and state banking and securities regulators, the Federal Reserve, the Office of the Comptroller of the Currency (OCC), and the U.S. Treasury Department's Office of Foreign Assets Control (OFAC)

EU

In the European Union (EU), the Markets in Crypto-Assets (MiCA) Regulation provides a detailed framework for stablecoins, but deposit tokens issued by licensed credit institutions are generally excluded from MiCA's requirements for Electronic Money Tokens (EMTs) and Asset-Referenced Tokens (ARTs), remaining under the established banking regulatory perimeter.

UK

Similarly, the United Kingdom (UK) treats bank-issued deposit tokens as traditional bank liabilities, with the Bank of England (BoE) focused on managing the potential systemic risk of deposit outflows to digital monies, particularly those associated with the ongoing Tokenised Sterling Deposits industry pilot

Singapore

In Singapore, the Monetary Authority of Singapore (MAS), regulates deposit tokens under existing banking laws (Banking Act). They are distinct from the stablecoin regulatory framework, which applies to non-bank issued single-currency stablecoins. However, deposit tokens may fall within the ambit of digital payment tokens under the Payment Services Act 2019 depending on how they are structured and used.

Hong Kong

In Hong Kong, the Hong Kong Monetary Authority is actively exploring tokenized deposits through initiatives like Project Ensemble, which is testing the use of tokenized deposits alongside a potential CBDC. Deposit tokens are treated as liabilities of Authorized Institutions (AIs), requiring them to comply with all existing banking and consumer protection standards.

Japan

Japan regulates tokenized deposits as a form of Electronic Payment Instrument (EPI) under the Payment Services Act (PSA), allowing licensed banks and trust companies to issue them, with strict rules on 1:1 reserve backing and segregation of funds.

V) CONCLUSION

Future considerations for payments systems using stablecoins, CBDCs, and deposit tokens as digital money will rely on current developments in regulatory frameworks and standards. Regulatory clarity, including consumer protections, will continue to evolve with rules specific to each form of digital money, and provisions for liability and accountability in the case of unwanted events. Payment systems will therefore require rails harmonized with these regulatory and standards developments.

While the United States has clearly taken a stance favoring stablecoins – particularly supporting regulatory clarity for USD-backed stablecoins, other jurisdictions - notably the EU - favor CBDC models which may compete with stablecoins. This may lead to a future where privately issued and sovereign issued forms of money compete and coexist and create new economic dynamics.

As blockchain rails converge with traditional rails, we're heading toward a global multi-rail world where deposit tokens, public or private stablecoins, and one or multiple CBDCs will coexist. Payment systems will require interoperability layers so a user can pay in one form (e.g., stablecoin) and a merchant can receive in another (e.g., CBDC or deposit token). Future payment systems will look more like routers/orchestration layers than single monolithic rails.

RECOMMENDATIONS

1. Harmonize Regulatory Frameworks Across Jurisdictions to minimize fragmentation, promote seamless global payments, and enable fungibility of digital money across markets

- Mutual recognition of compliant fiat-backed digital money should be treated equally
- Convergence toward the "same activity, same risk, same regulation" approach should ensure equivalent oversight for equivalent payment functions
- Alignment of travel rule, AML/CFT, and licensing standards to support cross-border interoperability

2. Establish Clear Standards for On/Off-Ramps, closing standards gaps to support compliance and minimize fragmentation

- Globally accepted requirements for minting/burning, reserve reconciliation, reporting, and transparency
- Uniform requirements for reserve audits, liquidity management, and segregation of funds across issuers

3. Standardize a Digital Identity layer and KYC for Blockchain-Based Payments for greater portability, privacy, and compliance

- Integrate digital identity credentials (e.g., vLEI, national ID systems, KYC frameworks) with wallet onboarding
- Adopt privacy-preserving identity models compatible with AML/CFT, avoiding on-chain PII and enabling verifiable compliance
- Wallet initialization standards (e.g., whitelisting, verification tiers, and key-management requirements)

4. Develop Interoperability Frameworks Across Digital Money Types, preparing for a multi-rail world where many forms of money will interoperate (e.g., payer sends one form of digital money and receiver can receive another)

- Implement interoperability bridges and secure asset transfer protocols (e.g., SATP, IEEE interoperability standards)
- Support atomic settlement across money types, especially for FX
- Create uniform token standards for settlement between rails (e.g., cross-chain TTF extensions, ERC-1400/3643-style compliance layers)

5. Strengthen Standards for Clearing, Settlement, and Reconciliation to reduce operational risk and align settlement on the blockchain with established financial market standards.

- Define canonical settlement rules for each digital money model, especially for atomic settlement
- Standards for FX rate determination, liquidity pools, and cross-currency settlement for stablecoins, CBDCs, and deposit tokens
- Requirements for reconciliation between wallets, blockchain ledgers, and omnibus accounts

6. Formalize Risk Mitigation Standards for Smart Contracts (e.g., security, upgrades, governance)

- Standardized smart-contract audit requirements (e.g., code scanning, formal verification, upgrade procedures)
- Governance rules for pausing transfers, freezing assets, and clawback mechanisms
- Build on existing frameworks for payment-specific contract governance standards

7. Improve AML/CFT Traceability While Preserving User Privacy

- Off-chain encrypted data-sharing networks for Travel Rule compliance
- Selective disclosure and zero-knowledge proof attestations for KYC, source-of-funds, and sanctions checks
- Risk-segmented wallet structures, (as some VASPs already use), to handle high-risk and low-risk funds separately

8. Establish Governance Models for Reversals, Disputes, and Consumer Protection, as governance is key for mainstream adoption

- Clear operational rulebooks for error handling, consumer disputes, and fraud claims
- Standards for reversible transactions (e.g., tagged transactions, hash-linked metadata, timelocks)
- Standardize clawback governance models for VASPs and custodians.

9. Promote Institutional-Grade Infrastructure for Deposit Tokens and Stablecoins

- Institutional-grade custody, treasury integration, settlement workflows, and role-based permissions
- ERP and corporate treasury integrations for automated on-chain cash management
- Multi-rail treasury systems compatible with existing payment standards and blockchain rails

10. Establish Collaborative Standards Working Groups, as collaboration is essential to prevent fragmentation and ensure scalability

- Public-private technical working groups bringing together central banks, banks, VASPs, standards bodies (ISO/ITU/IEEE), and blockchain communities
- Harmonize standards across all stages of the payments lifecycle
- Transition industry-driven blockchain standards into formally recognized global standards

OPEN QUESTIONS

- What information should be stored on-chain, and what must remain off-chain?
- For off-chain data, what storage models and security mechanisms should be required?
- What is the right balance between privacy and compliance—and should that vary by use case?
- How should interoperable information flows be facilitated across stakeholders?
- How should digital identity be standardized across all forms of digital money?
- How should requirements for digital money models be aligned across stablecoins, CBDCs, and deposit tokens, and potentially other forms of digital money?
- How should requirements be aligned across jurisdictions to support seamless global payments?
- What interoperability standards should govern multi-rail payments (across blockchain/banking/CBDC rails)?
- How should FX rates, cross-currency settlement, and liquidity be standardized?
- What governance model should define reversals, refunds, and dispute resolution?
- How should liability be distributed across issuers, wallets, VASPs, and networks?
- How should risk scoring and AML monitoring be standardized across chains and off-chain financial systems?
- How should settlement finality be defined in networks that can fork, reorganize, or pause?
- What global security standards should govern smart contracts?
- What consumer protection requirements are necessary for mainstream adoption?
- How should integration layers be designed for real-world deployments?

ENDNOTES

DIGITAL MONEY & WALLETS

1 Does not include non-blockchain DLTs, or hybrid ledgers.
2 https://www.theblock.co/post/373314/stablecoin-market-cap-surpasses-300-billion-for-first-time-amid-crypto-rebound
3 https://www.pwc.com/m1/en/publications/2025/docs/unlocking-the-future-of-finance-with-stablecoins.pdf
4 https://www.pwc.com/m1/en/publications/2025/docs/unlocking-the-future-of-finance-with-stablecoins.pdf
5 https://www.jpmorgan.com/insights/global-research/currencies/stablecoins
6 Coinmarketcap data as of Nov 28, 2025
7 https://www.theblock.co/post/377031/jpmorgan-circle-usdc-stablecoin-tether-usdt-onchain-growth
8 https://www.atlanticcouncil.org/cbdctracker
9 https://www.atlanticcouncil.org/cbdctracker
10 https://www.gi-de.com/en/spotlight/currency-technology/cbdc-its-time-to-act
11 https://www.atlanticcouncil.org/cbdctracker
12 https://www.jpmorgan.com/kinexys/documents/deposit-tokens.pdf
13 https://kpmg.com/xx/en/our-insights/value-creation/deposit-tokens-bridging-traditional-banking-and-the-digital-economy.html
14 https://www.forbes.com/sites/digital-assets/2025/09/09/real-world-assets-nearly-died-now-theyre-soaring-in-crypto/
15 https://www.addx.co/files/bcg_ADDX_report_Asset_tokenization_trillion_opportunity_by_2030_de2aaa41a4.pdf
16 https://www.mckinsey.com/industries/financial-services/our-insights/the-stable-door-opens-how-tokenized-cash-enables-next-gen-payments
17 https://eur-lex.europa.eu/eli/dir/2015/2366/oj/eng
18 https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money
19 https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng
20 https://eur-lex.europa.eu/eli/dir/2018/843/oj/eng
21 https://www.fatf-gafi.org/en/publications/Fatfgeneral/Guidance-rba-virtual-currencies.html
22 https://assets.ctfassets.net/so75yocayyva/4Plcwx7j9lfGuLHUnvnFKW/864b0955a33ab1467d2971825f7273ae/Proposed_Risk_Mitigation_Framework_for_Non-Financial_Risks_of_Blockchain_Infrastructure.pdf
23 https://datatracker.ietf.org/doc/rfc8578/
24 https://cdn.prod.website-files.com/648841abc97f28489cc3f2ce/6656e9c60c3029989dcd7431_IVMS101.2023%20interVASP%20data%20model%20standard.pdf
25 https://sagroups.ieee.org/bdlsc/

26 https://notabene.id/tap
27 https://notabene.id/tap
28 https://eur-lex.europa.eu/eli/dir/2015/2366/oj/eng
29 https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money
30 https://datatracker.ietf.org/doc/rfc8578/
31 https://datatracker.ietf.org/doc/draft-ietf-satp-architecture/
32 https://assets.ctfassets.net/so75yocayyva/4Plcwx7j9lfGuLHUnvnFKW/864b0955a33ab1467d2971825f7273ae/Proposed_Risk_Mitigation_Framework_for_Non-Financial_Risks_of_Blockchain_Infrastructure.pdf
33 https://assets.ctfassets.net/so75yocayyva/4Plcwx7j9lfGuLHUnvnFKW/864b0955a33ab1467d2971825f7273ae/Proposed_Risk_Mitigation_Framework_for_Non-Financial_Risks_of_Blockchain_Infrastructure.pdf
34 https://assets.ctfassets.net/so75yocayyva/4Plcwx7j9lfGuLHUnvnFKW/864b0955a33ab1467d2971825f7273ae/Proposed_Risk_Mitigation_Framework_for_Non-Financial_Risks_of_Blockchain_Infrastructure.pdf
35 https://www.frbservices.org/financial-services/fednow/what-is-iso-20022-why-does-it-matter
36 Definitions below come from CFTC – GMAC – DAMS taxonomy: https://www.cftc.gov/media/10321/CFTC_GMAC_DAM_Classification_Approach_and_Taxonomy_for_Digital_Assets_030624/download&sa=D&source=editors&ust=1755814393564217&usg=AOvVaw3gDYhL95fgP0FusGMzpkkk
37 Source: coinmarketcap, as of Nov 26, 2025 noting that market capitalization as an indication of size an adoption may reflect market dynamics more than payments utility.
38 https://zodia-custody.com/singapores-bold-approach-to-regulating-digital-assets/
39 https://www.mas.gov.sg/schemes-and-initiatives/project-guardian

GBBC