OST
Eastern Switzerland
University of Applied Sciences

Analysis of Swiss Stablecoin: “How to meet Swiss AML/CFT Goals in the context of a Stablecoin”

This paper provides a comprehensive analysis of the regulatory requirement for stablecoin issuers in Switzerland to adopt a whitelisting approach to ensure complete compliance with the Anti-Money Laundering Act (AMLA). Initially, the rationale behind FINMA’s stringent whitelisting requirements is thoroughly examined, clearly outlining the specific AML risks the regulator aims to mitigate. Subsequently, the study critically evaluates several alternative compliance mechanisms – including blacklisting, transaction monitoring, conditional time-delayed transfers, and identity verification via zero-knowledge proofs – assessing their compatibility with Swiss AML standards. The residual risks inherent in these alternatives are meticulously detailed, alongside proposed technical, operational, and regulatory mitigation strategies. Furthermore, the paper presents a comparative legal analysis of stablecoin compliance mechanisms employed in key jurisdictions such as the United States, the United Kingdom, the European Union, and Singapore, offering valuable international context. The analysis concludes by rigorously assessing the overall feasibility of these alternative mechanisms within the Swiss legal framework, addressing civil law considerations related to blocking, freezing, and withdrawal of tokens, as well as criminal procedural aspects concerning asset seizure pursuant to Article 263 StPO.

Contents

1. Introduction

Stablecoins have rapidly emerged as a pivotal link between traditional finance and the digital asset ecosystem. These tokens peg their value to fiat currencies or other assets, aiming to combine the stability of familiar units (like the US dollar, the Euro or the Swiss franc) with the transactional benefits of cryptocurrencies. This dual nature – bridging traditional finance and the digital asset ecosystem – has led to significant growth in stablecoin adoption for payments, trading, and remittances. It has also drawn increasing scrutiny from regulators concerned with financial stability, consumer protection, and AML/CFT risks.

Swiss regulators view stablecoins as carrying significant risks, especially regarding money laundering and illicit finance due to their price stability and global transferability. In response, the Swiss Financial Market Supervisory Authority (FINMA) has issued guidance and interpretations to clarify how existing laws (e.g. anti-money laundering, banking) apply to stablecoin issuers. Notably, FINMA's Guidance 06/2024 asserts that any institution issuing stablecoins in Switzerland is a financial intermediary under the Anti-Money Laundering Act (AMLA) and must ensure full compliance with due diligence requirements.

However, regulatory responses to stablecoins are evolving globally. In particular, the European Union's Markets in Crypto-Assets (MiCA) framework represents one of the first comprehensive regimes for crypto-assets, including stablecoins. MiCA, which took effect in stages through 2024, imposes strict requirements on stablecoin issuers to enhance transparency and safety – such as mandating full reserve backing and requiring issuers to obtain a license (e.g. as a bank or electronic money institution).

The scope of this analysis spans such international developments and their implications for Switzerland. We examine various stablecoin models – from those operating in regulatory gray areas to fully regulated instruments – and assess how emerging rules influence their design. Of special interest is how stablecoins integrate compliance measures (for example, on-chain KYC/AML controls to prevent illicit use) and how jurisdictions like Switzerland might respond to or adopt elements from frameworks like MiCA. The goal is to provide a clear understanding of the current stablecoin landscape and to outline how Swiss regulatory perspectives align with, or diverge from, these global trends.

2. Swiss Regulatory Framework for Stablecoins

In Switzerland's legal framework, the treatment of a stablecoin depends on its structure and use. FINMA's 2019 guidance (an ICO Guidelines supplement) stated that stablecoins are "almost always" subject to AMLA as means of payment, and that if a stablecoin grants a redemption claim against the issuer, it may even constitute a banking deposit. FINMA reiterated in 2024 that stablecoins often involve a holder having a claim on the issuer redeemable at face value – which can legally be a deposit unless special structuring (e.g. a bank guarantee) is used. Thus, a stablecoin issuer in Switzerland potentially faces two parallel regulatory regimes:

2.1 Banking Law

If the stablecoin represents a repayable claim (redeemable 1:1 for fiat at any time), the issuer may be taking deposits from the public. Under the Bank Act, taking public deposits requires a banking license unless an exemption applies. FINMA's Guidance 06/2024 warns that issuing a stablecoin redeemable at par triggers banking regulation, deemed "overkill" by commentators but mandated by current law. A common workaround to circumvent the banking license requirement involves a bank guarantee exemption under art. 5(3)(f) Banking Ordinance. Here, a licensed bank explicitly guarantees the issuer's redemption obligations, with conditions mandated by FINMA, such as individual customer claims against the guarantor bank and swift payouts upon issuer default.

2.2 Securities and DLT Law

Depending on structure, a stablecoin may also be treated as a security ("Effekte") or uncertificated security under the Swiss Code of Obligations and the new DLT-framework. If the token embodies a claim or entitlement (e.g. a bond or derivative form), it could be a security requiring a prospectus for offers or other securities law compliance. For example, a stablecoin structured as a tokenized bond (granting a debt claim) would be a security and could be issued as a ledger-based security ("DLT-Security") under the 2021 DLT law reforms. In contrast, if a stablecoin is purely algorithmic with no issuer claim, it might be treated like a cryptocurrency (not a security) but still often falls under AML rules if used for payments. FINMA has indicated that even when not securities, stablecoin issuers are financial intermediaries subject to AML requirements whenever they engage in token issuance, redemption, or storage for customers.

2.3 FINMA AML Requirements

Swiss anti-money laundering law imposes strict Know-Your-Customer (KYC) and Customer Due Diligence (CDD) obligations on all financial intermediaries, including issuers of stablecoins. This means before establishing a business relationship or executing certain transactions, the issuer must verify the customer's identity, identify beneficial owners, and monitor for suspicious activity. Historically, for cryptocurrencies, FINMA followed a "intermediary-centric" approach: KYC/AML checks were required at on-ramps/off-ramps (e.g. when

a regulated entity sells or redeems tokens for fiat), but purely peer-to-peer transfers without an intermediary were not directly regulated. However, stablecoins have prompted a much stricter interpretation by FINMA in 2021 and 2024. According to FINMA's 2021 Annual Report and reaffirmed in Guidance 06/2024, issuers must ensure that all persons holding or transacting in the stablecoin are identified – not just the initial purchaser or redeemer. In practice, FINMA expects stablecoin arrangements to incorporate contractual or technological transfer restrictions so that the token cannot be passed to unknown parties. This is essentially a ban on anonymous usage: even intermediate holders in secondary market transfers must be known to the issuer or an authorized intermediary. FINMA analogizes this to the long-standing Swiss ban on anonymous bearer savings accounts, extending that principle into the crypto realm. The regulator views the relationship between a stablecoin issuer and any holder of its coin – even if there's no direct contact – as a "permanent business relationship" under AML regulations, a contentious interpretation that goes beyond the letter of the law.

2.4 Implications

As of today, the Swiss regulatory stance is uniquely strict. FINMA's guidance effectively mandates a "whitelist" approach for stablecoins: only approved, KYC-verified addresses or users should be able to hold or transact the coin. This goes further than international standards and has been described as regulatory overreach or "Swiss gold-plating" of AML rules. FINMA justifies it on reputational risk and policy grounds (preventing illicit flows), noting that stablecoins have been used in sanctions evasion (e.g. conflict zones) and thus pose acute AML risks.

Nevertheless, industry experts argue that no other major jurisdiction – not the EU, U.S., UK, Singapore, nor the FATF's global standards – requires identification of all downstream holders for every stablecoin transfer. This stringent Swiss approach makes it de facto difficult to issue a freely transferable stablecoin in Switzerland without heavy controls. Indeed, legal commentators conclude that under the current framework it is "impossible to issue a stablecoin in a manner that makes sense economically" in Switzerland, and suggest new legislation is needed to recalibrate these requirements. The Swiss State Secretariat for International Finance (SIF) is reportedly working on proposals (e.g. as part of fintech license reforms) to update stablecoin regulations in the near future.

3. Compliance Mechanisms: Whitelisting vs. Alternative Approaches

Given FINMA's stance, Swiss stablecoin issuers must carefully design compliance controls into the token's functionality. The traditional mechanism has been address-whitelisting, but various alternative or complementary approaches exist. This section evaluates the legal feasibility and regulatory acceptance in Switzerland of different mechanisms to meet AML/KYC goals:

3.1 Whitelisting

This is the FINMA-endorsed solution. Only addresses or accounts that have undergone KYC verification are permitted to transact in the stablecoin. Technologically, this can be implemented via smart contract logic that checks a list of authorized addresses before allowing transfers. For instance, Sygnum Bank's DCHF stablecoin employs an integrated whitelist in its ERC-20 smart contract to ensure only whitelisted addresses (belonging to identified Sygnum clients or partners) can send or receive DCHF. Whitelisting guarantees that at any point, the issuer knows the identity of current holders, thereby satisfying FINMA's requirement that "all persons disposing of stablecoins" are identified. The downside is reduced fungibility and interoperability – the coin cannot freely circulate on public blockchain networks, undermining some benefits of crypto.

From a legal perspective, whitelisting is feasible and in fact expected in Switzerland. FINMA explicitly "requires that transfers to persons not on the whitelist be restricted by contractual and/or technical means". Thus, any Swiss issuer not implementing a whitelist would likely fail to meet current supervisory expectations. The cost, however, is high friction: every new user must undergo onboarding, and peer-to-peer transfers are limited to pre-approved participants or through regulated VASPs (Virtual Asset Service Providers).

3.2 Blacklisting

A more permissive alternative is to allow open transfers but maintain the ability to blacklist certain addresses associated with fraud, sanctions, or other illicit activity. Under a blacklisting model, anyone can initially receive the stablecoin, but the issuer (or smart contract admin) can later freeze addresses that are identified as suspicious, preventing further transfers or redemptions from those addresses. This approach is used by major global stablecoins like USD Coin (USDC) and Tether (USDT) under U.S. jurisdiction – for example, Centre (the consortium behind USDC) has blacklisted addresses linked to theft or sanctions, locking up those funds.

Legally, blacklisting is less proactive than whitelisting: it does not stop an illicit transfer from occurring but intervenes only afterward, by permanently freezing tokens held at problematic addresses. This distinguishes blacklisting from mere transaction-level (also preventive) blocking, which typically involves temporarily halting specific transfers (pending further checks) rather than permanently immobilizing an entire address. FINMA's

current posture suggests blacklisting alone would not satisfy Swiss AML requirements, because it does not ensure upfront identification of all token holders. FINMA wants no transfers to unknown parties at all, whereas blacklisting inherently assumes transfers are permitted until a problem is identified.

In Swiss AML terms, blacklisting could thus be viewed as too reactive to fulfill the due diligence duty of verifying counterparties before a transaction occurs. Consequently, FINMA explicitly requires upfront identification of all token holders, deeming blacklisting insufficient on its own due to its purely retrospective nature. FINMA's 2024 guidance implicitly rejects anonymous circulation models with ex-post freezing alone, insisting instead on preventive restrictions such as whitelisting. Nevertheless, blacklisting may still function effectively as a supplementary compliance measure: for instance, even within a whitelisted system, an address may subsequently need to be blacklisted if the user's status changes (e.g., becoming sanctioned). Therefore, Swiss issuers should ensure explicit contractual terms reserving the right to permanently freeze or blacklist addresses as required, aligning with regulatory expectations and sanctions compliance obligations.

3.3 Active Transaction Monitoring

This mechanism entails closely monitoring all transactions on the stablecoin network for suspicious patterns (using blockchain analytics and AML software), combined with intervention when necessary. An issuer could choose not to whitelist every address, but instead permit open access while monitoring flows, filing suspicious activity reports (SARs) and freezing tokens when a high-risk or illicit activity is detected. Modern analytics can flag transactions associated with darknet markets, mixers, or sanction-hit wallets.

In Switzerland, all financial intermediaries must monitor for suspicious transactions and report them to the Money Laundering Reporting Office (MROS) if suspected (Swiss AMLA Art. 9). If a report is made, the intermediary must freeze the assets for a short period (up to 5 days) awaiting authorities' decision. Thus, in theory, a stablecoin issuer could comply by monitoring and freezing as required by AMLA without necessarily pre-approving every holder. However, FINMA is dubious of this approach for stablecoins. The regulator's concern is that once a token has moved to an unknown party, tracing and enforcing compliance becomes difficult. While continuous monitoring is essential even in whitelisted systems, using it as the primary control (in lieu of whitelisting) is not deemed sufficient under current Swiss practice. FINMA's guidance implies that preventing illicit transfers in the first place is preferred over relying on detection after the fact.

Legally, nothing in Swiss law explicitly forbids a monitor-and-freeze approach – it could be argued to satisfy the letter of AMLA (identifying customers when establishing business relationships and freezing/reviewing suspicious transactions). But given FINMA's explicit guidance to restrict all non-whitelisted transfers, any issuer proposing only ex-post monitoring would likely face supervisory rejection. In short, transaction monitoring is mandatory but not an adequate standalone replacement for upfront KYC in the Swiss stablecoin context.

3.4 Zero-Knowledge Proofs

A novel idea is deploying cryptographic protocols that prove a user is authorized (KYC-verified) without revealing their identity on-chain. For example, a stablecoin system could integrate a zero-knowledge proof (ZKP) scheme where users obtain a proof of KYC from a trusted verifier, and the smart contract allows transfers if both sender and receiver present valid proofs. This would essentially implement whitelisting but in a privacy-enhanced way – the blockchain might not list the addresses on a public whitelist, but each transaction carries a hidden credential showing compliance.

From a legal perspective in Switzerland, ZKPs are intriguing because they could satisfy the spirit of FINMA's rule (only identified persons transact) while mitigating privacy concerns. FINMA has not explicitly opined on ZK proofs in this context yet. The likely requirement would be that the system's design is audited or certified such that FINMA takes comfort that only compliant users can use the coin. If the issuer or an intermediary still knows the identity behind each credential (even if the chain does not broadcast it), this could be acceptable. As such, ZKPs theoretically fulfill FINMA's identification requirements while protecting privacy.

As of today, no Swiss stablecoin has publicly implemented a ZKP-based compliance model, and FINMA's guidance does not mention it. However, FINMA emphasizes technology-neutrality – in principle, any technological solution that ensures AML requirements are met could be allowed. A law firm commentary on Guidance 06/2024 suggests advanced solutions (like limiting transfers to VASPs or whitelisted groups via technology) might fulfill the rules without literal ID of each holder by the issuer, provided the outcome is the same. Thus, a well-designed zero-knowledge system could be legally feasible if it demonstrably blocks unknown, non-KYC'd users. It would require FINMA's buy-in and likely significant assurance testing. In summary, ZKP compliance mechanisms are theoretically feasible under Swiss law (nothing prohibits them) and could one day reconcile FINMA's AML demands with user privacy, but they remain untested and would need regulator engagement to be accepted.

3.5 Delayed Transfers / Advance Notice Mechanisms

Another possible mechanism is imposing a time delay on token transfers – for example, any on-chain transfer only executes after a certain period (say 24 hours) during which the issuer is alerted and can vet the transaction. If during that window an issue is detected (e.g. destination is unverified or blacklisted), the issuer could halt the transfer. This is somewhat analogous to how some exchanges implement withdrawal hold periods for security. Under a delay scheme, the stablecoin could technically be more open (not strictly whitelisted), yet still offer the issuer a chance to intervene on problematic transactions before finality.

Swiss law does not forbid contractual terms that make token transfers subject to delay or approval – indeed, this could be seen as a "technical transfer restriction" consistent with FINMA's guidance. FINMA might view

delayed transfers as better than unrestricted transfers, but still not as ideal as outright whitelisting. A delay plus review essentially shifts the model closer to a banking system where transactions clear only after screening. This could satisfy AML checks (the issuer would ensure the recipient is identified during the delay), thus meeting the requirement that unknown parties do not end up with the stablecoin. However, such friction severely hampers usability for real-time transactions and may not be commercially attractive.

As of today, no prominent Swiss project uses an on-chain delay mechanism for compliance. It remains legally possible – an issuer could include in its token smart contract that any transfer to a new address triggers a hold until approved – but the regulatory acceptance would likely hinge on proving this reliably stops illicit transfers. FINMA might question whether the issuer can truly identify the counterparty within the delay unless the counterparty proactively registers. In practice, delayed execution might just be a slower form of whitelisting (i.e. every new address gets approved during the delay). Therefore, while possible, delayed transfers are an unconventional solution that would need FINMA's explicit comfort to be viable.

3.6 Summary of Swiss Position on Alternatives

FINMA's current policy leaves little room for anything short of full upfront identification of all stablecoin users. Approaches like blacklisting or pure monitoring, which are accepted in other jurisdictions, are not sufficient under FINMA's "identify-all-holders" interpretation. Innovative solutions like ZK proofs or time delays could theoretically achieve the same end and might be considered technology-neutral equivalents, but they would need to be proven to regulators.

Therefore, at present, whitelisting remains the only clearly acceptable mechanism to satisfy Swiss AML for stablecoins. Alternative compliance mechanisms, while legally feasible, face a high bar for regulatory approval in Switzerland's cautious environment.

4. Comparative AML/KYC Requirements in Other Jurisdictions

Switzerland's stance on stablecoin compliance can be contrasted with approaches in the United States, United Kingdom, European Union, and Singapore. These jurisdictions all impose AML/KYC obligations on crypto businesses, but none require the blanket identification of every token holder that Switzerland does. Below is a brief legal comparison focusing specifically on AML/KYC for stablecoin issuers:

4.1 United States

As of 2025, the United States does not yet have a bespoke federal regulatory framework specifically governing stablecoins, although several legislative proposals are under active consideration. In the absence of a dedicated law, stablecoin issuers currently operate under a combination of existing federal financial regulations and individual state licensing regimes. Efforts to introduce federal legislation, including the Clarity for Payment Stablecoins Act (also known as the McHenry-Waters Act), the Stablecoin TRUST Act, and the Genius Act, reflect growing bipartisan recognition of the need for tailored regulation, particularly to address reserve quality, issuer licensing, and redemption rights. However, until such legislation is passed, regulatory compliance is primarily derived from existing AML and money transmission rules.

4.1.1 FinCEN Regulations

The U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) treats most fiat-backed stablecoin issuers as Money Services Businesses (MSBs) if they issue or redeem tokens convertible to fiat currency. As MSBs, stablecoin issuers must register with FinCEN and comply with the Bank Secrecy Act (BSA), including its "four pillars" of AML compliance: written policies and procedures, designation of a compliance officer, employee training, and independent testing of the program. Additionally, MSBs must implement a Customer Identification Program (CIP) to verify the identity of customers at the point of onboarding.

Importantly, U.S. AML obligations apply only to direct counterparties—that is, those who acquire or redeem tokens directly from the issuer. Stablecoin issuers are not required to identify or monitor individuals who acquire tokens on the secondary market. This principle was reaffirmed in FinCEN's 2019 guidance on virtual currencies, which clarified that AML obligations attach to the MSB's activities, not to peer-to-peer transfers beyond its operational control. For instance, if Alice purchases USDC from Circle, Circle must KYC Alice. If Alice later transfers that USDC to Bob via a personal wallet, Circle bears no compliance obligation toward Bob under current federal rules. This "endpoint-based" AML model stands in contrast to Switzerland's all-holders KYC requirement and highlights the U.S. emphasis on risk-based compliance at regulated touchpoints, not continuous token-level enforcement.

4.1.2 State Licensing and Controls

Many stablecoin issuers seek state-level licenses to operate legally across jurisdictions. For example, Paxos and Gemini operate under the New York Department of Financial Services (NYDFS) framework, which includes the BitLicense or limited-purpose trust charters. These licenses impose stringent capital, audit, AML, and cybersecurity requirements, including regular supervisory examinations.

Despite the absence of a national whitelisting mandate, most U.S.-based issuers implement blacklist functionality to meet obligations under U.S. sanctions law. Pursuant to the Office of Foreign Assets Control (OFAC) regulations, issuers must block assets held by sanctioned individuals or entities, treating such funds as "blocked property". In practice, this means maintaining smart contract-level capabilities to freeze (or nullify) stablecoins held at specific addresses. For example, Circle and Tether have routinely complied with OFAC designations by freezing tokens at addresses flagged for links to ransomware, terrorist financing, or fraud. U.S. law enforcement agencies can also obtain seizure or forfeiture orders covering stablecoin balances, which are executed with the cooperation of the issuer or custodial platforms.

Several federal legislative proposals, such as the Stablecoin TRUST Act and the Clarity for Payment Stablecoins Act, envision codifying these practices into law, potentially requiring all federally regulated stablecoin issuers to maintain capabilities for token freezing, claw-backs, and redemption assurance. The Genius Act, introduced in 2024, similarly addresses reserve transparency and consumer protection, especially in relation to payment stablecoins. While no single bill has yet passed both chambers of Congress, a growing regulatory consensus supports enhanced oversight through issuer-based controls, rather than enforcing AML obligations directly at the protocol or wallet level.

4.1.3 Summary of U.S. Approach

The U.S. apply a pragmatic, issuer-centric AML framework to stablecoins. Issuers must comply with FinCEN registration, implement full KYC and AML programs for primary issuance and redemption transactions, and observe reporting requirements such as Currency Transaction Reports (CTR) and Suspicious Activity Reports (SAR). While federal legislation is pending, stablecoin issuers already operate under enforceable AML and sanctions compliance rules. Importantly, peer-to-peer stablecoin transfers remain lawful and unregulated, provided they do not involve a regulated intermediary.

The U.S. model emphasizes post-transfer monitoring, detection, and enforcement—including address freezing where required—rather than proactive whitelisting or universal KYC of all token holders. This risk-based

structure, built around regulated entry and exit points, reflects the country's broader reliance on institutional accountability and technological flexibility over transactional restriction.

4.2 United Kingdom

UK regulations integrate stablecoins into existing AML/CFT frameworks, requiring robust AML controls and KYC at issuance or redemption points but without mandating comprehensive whitelisting of all token holders. The Financial Services and Markets Act 2023 created a framework for "digital settlement assets" (including stablecoins) to be regulated, and the Bank of England (BoE) and Financial Conduct Authority (FCA) are working on detailed rules. As of 2025, the BoE and FCA are in the process of finalizing the detailed regulatory regime, which will cover authorization, prudential requirements, and conduct rules for stablecoin issuers and service providers. Key points related to AML/KYC requirements for stablecoins are highlighted in the following sections.

4.2.1 UK AML Regulations (MLRs)

Since January 2020, UK AML Regulations (MLRs) have required crypto-asset businesses (including exchanges, custodians, and potentially issuers if doing business in the UK) to register with the FCA and implement risk-based AML programs. A stablecoin issuer serving UK customers likely falls under this regime as a "crypto asset exchange provider" or "custodian wallet provider" if they facilitate transactions or custody or control user funds. This means UK authorities already mandate KYC for customers dealing directly with the issuer, but not for all subsequent holders.

4.2.2 UK FCA's 2023 Discussion Paper (DP23/4)

The FCA's 2023 Discussion Paper (DP23/4) on crypto assets outlines the future regulatory model for stablecoin issuers, who are expected to be authorized under a framework comparable to that for e-money or payment institutions. The paper confirms that issuers will be obligated to perform customer due diligence (CDD) when interacting directly with token holders, particularly at the point of issuance or redemption. For example, if a user seeks to redeem stablecoins for fiat, especially from an unhosted wallet, the issuer must conduct appropriate identity checks before processing the redemption. However, the FCA explicitly does not require identification of all intermediate holders trading the stablecoin in between these touchpoints. There is no blanket whitelisting obligation in UK law, and the regime is intentionally designed to be risk-based rather than fully restrictive.

4.2.3 Travel Rule in UK

The UK implemented FATF Recommendation 16, aka "Travel Rule" for crypto asset transfers in 2023, meaning that UK crypto firms, including those handling stablecoins, are required to collect and transmit originator and

beneficiary information for relevant transactions. This obligation applies when the transfer exceeds defined risk thresholds or involves a counterparty outside the UK. Unhosted wallet transactions are treated as higher risk under FCA guidance, and firms must conduct enhanced due diligence where appropriate. However, there is no outright prohibition on transfers to or from unverified self-custody wallets. KYC obligations are triggered only when those wallets interface with a regulated entity, such as during redemption or conversion through a UK-registered firm.

4.2.4 Summary of UK Approach

The UK regulatory approach seeks to embed stablecoins into the existing AML framework without creating unnecessary technological restrictions. Stablecoin issuers must register, implement robust AML programs, and identify their direct counterparties but they are not required to whitelist or pre-approve all token holders. The FCA and HM Treasury have both indicated that they do not support the all-holders identification model adopted by FINMA. Instead, the UK favors a risk-based model focused on issuer and intermediary conduct, allowing stablecoins to circulate freely within a framework of regulatory accountability at key access points.

4.3 European Union

The EU adopted the Markets in Crypto-Assets Regulation (MiCA) in June 2023, establishing the first comprehensive EU-level regulatory framework for crypto-assets. MiCA classifies stablecoins as either Asset-Referenced Tokens (ARTs), which reference baskets of assets or non-fiat values, or E-Money Tokens (EMTs), which are pegged to a single fiat currency (e.g., EUR or USD). The core MiCA provisions governing EMTs and ARTs entered into effect in June 2024, with transitional arrangements extending into early 2025 for certain actors.

MiCA is accompanied by related legislation under the EU's Anti-Money Laundering (AML) package, including the AML Regulation (EU) 2024/1624, the Sixth AML Directive (AMLD6, Directive 2024/1640), and the creation of the Anti-Money Laundering Authority (AMLA). These frameworks together impose strict compliance, governance, and transparency obligations on crypto-asset issuers and service providers operating within the EU.

4.3.1 Issuer Authorization

Under MiCA, the issuance of stablecoins to the public within the EU is strictly regulated. For EMTs the issuer must be an authorized electronic money institution (EMI) or credit institution under EU financial services law. This requirement brings with it substantial prudential, operational, and AML obligations, including minimum capital requirements, governance controls, and clear redemption rights for token holders. For ARTs a dedicated licensing regime has been created. Issuers of ARTs must apply for authorization from a competent national authority, submit an approved crypto-asset white paper, and meet specific capital, governance, and

business continuity standards. Issuers of both EMTs and ARTs are considered regulated financial entities, subject to direct supervisory oversight and full integration into the EU's AML/CFT regime. Together, these provisions aim to ensure that any entity offering stablecoins in the EU operates with financial soundness, transparency, and the capacity to uphold consumer and market integrity.

4.3.2 AML Requirements

MiCA explicitly mandates that stablecoin issuers and crypto-asset service providers comply fully with existing and newly adopted EU AML/CFT legislation. Specifically, Regulation (EU) 2024/1624 ("EU AML Regulation"), formally adopted in May 2024 as part of a comprehensive AML legislative package alongside the Sixth AML Directive (AMLD6) and the EU AML Authority (AMLA) Regulation, sets binding rules across the European Union. From December 2024, crypto-asset service providers (CASPs) and stablecoin issuers must adhere to detailed AML requirements, including mandatory compliance with the Travel Rule under the revised Funds Transfer Regulation. This Travel Rule obliges CASPs to collect, verify, and exchange originator and beneficiary information for all crypto transactions, effectively prohibiting anonymous accounts and enhancing transparency.

Operationally, this AML framework requires issuers and intermediaries to apply robust customer due diligence at onboarding, conduct ongoing transaction monitoring, and promptly report suspicious activities. Importantly, however, the AML Regulation does not mandate the identification of every token holder in intermediate peer-to-peer transfers; instead, the issuer's AML obligations focus primarily on direct interactions with their customers during issuance or redemption processes. Service providers handling stablecoin transactions remain responsible for compliance within their direct customer relationships, thereby ensuring effective AML/CFT control without universally mandating holder whitelisting.

4.3.3 Travel Rule in EU

The EU has revised its Transfer of Funds Regulation (TFR) to apply the Travel Rule to crypto-asset transfers, aligning with FATF Recommendation 16. As of 30 December 2024, all crypto transfers involving at least one regulated CASP in the EU must include complete originator and beneficiary information, with no minimum threshold. This requirement applies to all transactions, including those involving stablecoins, and mandates that CASPs collect and transmit this data to the next regulated institution in the transaction chain.

For transactions involving unhosted wallets, CASPs must collect identifying information for transfers above 1'000 Euro and conduct appropriate risk-based assessments. However, the EU did not adopt a full ban on unhosted wallets or their interaction with CASPs. As a result, while unhosted wallet activity remains permitted, it is subject to enhanced due diligence and monitoring obligations. Overall, the EU relies on regulated intermediaries and mandated information-sharing rather than embedding compliance directly into token

transfer mechanics. Unlike Switzerland, there is no requirement for stablecoin smart contracts to enforce whitelist-based restrictions.

4.3.4 Summary of EU Approach

EU's approach to stablecoin regulation under MiCA is generally considered stringent in terms of licensing, prudential oversight, and transparency requirements. Issuers of e-money tokens must be fully authorized financial institutions (EMIs or credit institutions), adhere to strict capital adequacy and reserve backing requirements, and maintain clear redemption mechanisms and public disclosures. Regulatory supervision by national competent authorities and ESMA ensures stablecoin stability and legal accountability.

In contrast to Switzerland's all-holders KYC interpretation under FINMA Guidance 06/2024, the EU does not require the identification of all token holders. Instead, AML/CFT controls are applied at regulatory touchpoints (issuance, redemption, and transfers through CASPs) supported by the Travel Rule and broader EU AML regulations. This means stablecoins may circulate between users without prior verification, as long as service providers comply with due diligence rules and report suspicious activity.

In short, the EU pursues a risk-based AML framework that entrusts compliance responsibilities to regulated institutions rather than embedding restrictions in token design. Stablecoin issuers must implement comprehensive AML programs, verify clients at onboarding, and cooperate with regulated intermediaries. However, the EU does not require technological whitelisting or identity enforcement at every point of token transfer, striking a balance between financial integrity and market usability.

4.4 Singapore

Singapore has embraced cryptocurrency innovation within a robust regulatory framework anchored in the Payment Services Act 2019 (PSA) and detailed guidance from the Monetary Authority of Singapore (MAS). In August 2023, MAS finalized its Stablecoin Regulatory Framework, applying to single-currency stablecoins (SCS) pegged to the Singapore Dollar (SGD) or G10 currencies. This framework complements broader digital payment token (DPT) regulation under the PSA and aims to ensure both stability and regulatory accountability.

4.4.1 Licensing and Scope

Under the PSA, activities involving stablecoins may fall into several licensing categories depending on the business model. The new MAS framework introduces a distinct regulated activity of "stablecoin issuance" for qualifying SCS, subjecting non-bank issuers to direct oversight with requirements covering reserve assets, prudential safeguards, disclosure obligations, and redemption protocols. Banks in Singapore are also permitted to issue SCS and are deemed already compliant with most regulatory requirements. Importantly, only those stablecoins issued in Singapore and fulfilling MAS's criteria can be marketed as "MAS-regulated

stablecoins." Other stablecoins such as "offshore tokens" can still circulate and be used but are treated as digital payment tokens (DPTs) under general crypto rules, without the regulatory label or guarantees attached to the SCS regime.

4.4.2 AML/CFT Obligations

Singapore imposes strict AML/CFT requirements on all DPT service providers, including exchanges, wallet providers, and under the stablecoin framework presumably also stablecoin issuers. MAS has confirmed that existing AML/CFT standards apply uniformly, including customer due diligence (CDD), transaction monitoring, sanctions screening, and Travel Rule obligations. Stablecoin issuers must perform KYC on customers who directly interact with them, such as purchasers or account holders, maintain records, and file suspicious transaction reports. The Travel Rule, in force since 2020 via MAS Notice PSN02, requires DPT service providers to transmit originator and beneficiary information for crypto transfers above defined thresholds when transacting with other regulated entities.

4.4.3 No Whitelist Requirement

Singapore does not impose a whitelisting requirement on all stablecoin users. Instead, MAS relies on a combination of licensing, AML/CFT compliance, and technology risk management. MAS's mentioned August 2023 stablecoin framework does not require token-level transfer restrictions. The focus is placed on issuer responsibility, value stability, and redemption assurances, rather than controlling token movement across the network. Stablecoins not qualifying under the framework may still be used in Singapore, but users do so at their own risk. Consistent with the EU and UK approach, Singapore requires issuers to monitor their direct relationships and comply with AML law but does not demand full identification of downstream holders. For instance, if a MAS-regulated stablecoin is traded on a decentralized exchange, the issuer is not obligated to identify each trader: responsibility lies with local intermediaries or arises at redemption.

4.4.4 Sanctions Compliance

Singapore enforces United Nations and domestic financial sanctions. MAS guidelines require all financial institutions, including stablecoin issuers, to identify and freeze assets belonging to sanctioned persons or entities. Therefore, a Singapore-based issuer must have the technical ability to blacklist or freeze specific addresses when required by law. These controls are not applied universally but serve as targeted enforcement tools to ensure compliance with sanctions, similar in approach to OFAC obligations in the U.S.

4.4.5 Summary of Singapore Approach

Singapore's regulatory regime is often seen as strict but proportionate, balancing innovation with financial system safeguards. It subjects stablecoin issuers to licensing, reserve, and compliance obligations while

avoiding overly restrictive measures that might stifle use cases. The MAS framework focuses on governance, redemption, and issuer accountability, not on enforcing universal on-chain identity controls. Singapore has explicitly noted that major jurisdictions do not require full identification of all stablecoin holders and has aligned its position accordingly. As long as issuers and intermediaries fulfill their AML/CFT responsibilities, including KYC, monitoring, and reporting, stablecoins may circulate freely in a controlled, but non-permissioned environment.

4.5 Summary of Comparative Analysis

In comparing these jurisdictions, it is clear that Switzerland continues to stand out for its exceptionally conservative approach to AML compliance for stablecoins. While the U.S., UK, EU, and Singapore all impose robust AML/CFT obligations on stablecoin issuers and regulated intermediaries, none require the stablecoin to operate exclusively on a closed, pre-approved network of users. These jurisdictions rely instead on a combination of issuer-level KYC controls, supervision of exchanges and wallet providers, and compliance with the FATF Travel Rule to mitigate illicit use.

Switzerland's whitelisting requirement for all token holders remains unique: no global standard, including those set by FATF, requires full pre-identification of all token recipients. This regulatory divergence has meaningful implications: it may incentivize Swiss-based projects to launch their stablecoins in more permissive foreign jurisdictions, or to lobby for Swiss rule changes to align with global practice.

The comparative view also illustrates the underlying regulatory trade-off: Switzerland emphasizes strict ex-ante prevention of anonymous usage, accepting potential frictions in technological innovation and market scalability. By contrast, other jurisdictions accept a degree of controlled anonymous circulation, focusing enforcement on entry and exit points, and strengthening compliance through monitoring, reporting, and sanctions. Each model reflects different policy priorities—Switzerland favoring maximum control, while others seek to balance financial integrity with innovation and practicality.

5. Selected Case Studies: Stablecoins and Compliance Mechanisms in Practice

To illustrate how these compliance mechanisms are implemented, this section examines real-life stablecoin projects and their approaches to AML/KYC in different legal contexts, including examples from Switzerland and abroad to illustrate the diverse approaches in design and regulatory compliance. We survey prominent examples of stablecoins and highlight how each navigates legal requirements and technical constraints.

Alongside well-established USD-pegged tokens, we include a Euro-denominated case study in a more comprehensive "deep dive": Societe Generale-FORGE's EUR CoinVertible (EURCV). Launched in 2023 by a major European bank, EURCV stands as one of the first stablecoins fully compliant with the EU's MiCA regulation. This token was initially available only to whitelisted, KYC-verified institutional participants, enforcing compliance through on-chain transfer restrictions. Notably, SG-Forge restructured EURCV in mid-2024 to meet MiCA's standards, achieving full Electronic Money Token (EMT) status and removing the prior whitelist so that transfers are now permitted between any addresses without pre-approval. Compliance controls remain integral, however: the EURCV smart contract empowers the issuer to pause transfers, freeze funds, or blacklist suspicious addresses in line with regulatory obligations.

By examining EURCV alongside other stablecoins, we can observe how regulatory alignment (in this case, with European law) can be built into a token's core mechanics, as such setting the stage for comparing such on-chain control models with more laissez-faire approaches, thereby underscoring the spectrum of strategies that stablecoin issuers employ to balance innovation with oversight.

5.1 USD Coin (USDC)

USD Coin (USDC) is a leading U.S. dollar-pegged stablecoin launched in 2018 by the Centre consortium, a collaboration between Circle and Coinbase. It rapidly became one of the most widely adopted stablecoins globally, known for combining regulatory compliance, transparency, and interoperability across various blockchain platforms, including Ethereum, Algorand, Solana, and others. USDC is issued by Circle Internet Financial, a licensed Money Services Business (MSB) registered with the Financial Crimes Enforcement Network (FinCEN), and holds multiple state-level licenses, including the stringent New York BitLicense.

5.1.1 Compliance and Regulatory Model

USDC is designed with compliance in mind, balancing openness and regulatory oversight effectively. The compliance structure involves both traditional off-chain controls and innovative on-chain enforcement mechanisms, providing a robust framework acceptable to regulators while retaining usability within decentralized finance (DeFi) ecosystems and general commerce.

5.1.1.1 Off-chain Compliance (KYC/KYB)

Circle and Coinbase require comprehensive Know-Your-Customer (KYC) and Know-Your-Business (KYB) procedures for all customers who directly mint (purchase) or redeem USDC through their platforms. These compliance checks adhere strictly to the Bank Secrecy Act (BSA) and related Anti-Money Laundering (AML) requirements, as mandated by FinCEN and state regulatory authorities. Institutional customers are subject to rigorous KYB checks, ensuring the transparency of entities involved in the issuance or redemption process. Moreover, secondary market users who acquire USDC through crypto exchanges are subject to KYC and AML procedures conducted by these regulated exchanges, extending compliance coverage across multiple layers of the USDC ecosystem.

5.1.1.2 On-chain Compliance Controls (Blacklisting and Freezing)

A distinctive feature of the USDC compliance model is its smart contract capability for on-chain enforcement. While the token is freely transferable across public blockchain networks – thus enabling wide accessibility and liquidity – it incorporates a built-in "blacklist" feature. This function allows Circle, as the primary issuer, to freeze USDC held at specific blockchain addresses deemed illicit or non-compliant.

This mechanism has been actively employed in coordination with U.S. law enforcement and regulatory agencies. Notably, in 2022, following the U.S. Treasury's Office of Foreign Assets Control (OFAC) sanctions on the cryptocurrency mixer Tornado Cash, Circle immediately froze approximately 75'000 USDC linked to addresses identified by OFAC. Circle has similarly intervened upon FBI requests in cases involving fraud or stolen assets, showcasing proactive compliance collaboration. These targeted interventions demonstrate that while USDC promotes open accessibility, it simultaneously equips regulators and law enforcement with effective tools for immediate and precise compliance enforcement.

5.1.2 Transparency and Reserve Management

Transparency is central to USDC's operational model. Circle publishes monthly attestation reports prepared by an independent auditor (currently Deloitte), confirming that all issued USDC tokens are fully collateralized by reserves held in segregated accounts. These reserves consist of U.S. dollar-denominated assets, typically cash and short-term U.S. Treasury securities, ensuring a stable and redeemable backing at a 1:1 ratio. Regular public disclosures and third-party attestations have significantly contributed to market trust and user confidence in USDC, distinguishing it from competitors with less transparent reserve management practices.

5.1.3 Regulatory Impact and Global Acceptance

USDC's "open-but-supervised" model has enabled broad global adoption, especially in DeFi platforms, crypto trading, and cross-border payments. Its balance of transparency, regulatory compliance, and ease of

integration has made it appealing to institutional investors, financial technology firms, and mainstream commerce. Regulators in the U.S. generally view USDC favorably as a compliant digital asset that aligns well with existing regulatory expectations.

However, its open transferability without mandatory initial identification of all holders contrasts with more stringent regulatory expectations found in jurisdictions such as Switzerland. For example, under current Swiss Financial Market Supervisory Authority (FINMA) guidelines, a stablecoin similar to USDC would need to incorporate whitelisting mechanisms, ensuring every token holder is identified prior to transacting. Thus, USDC's model, while compliant in the U.S. context, would require significant adaptation to satisfy Swiss AML/KYC standards fully.

5.1.4 Lessons and Implications

The success and broad acceptance of USDC provide important insights into effective stablecoin governance. Its compliance framework demonstrates how regulatory requirements can coexist with broad user accessibility and decentralization. The selective on-chain blacklisting approach highlights a middle ground, effectively managing AML and sanctions risks without resorting to comprehensive whitelisting. This approach aligns well with existing U.S. regulations and emerging global standards, suggesting that future regulatory frameworks might incorporate similar on-chain compliance capabilities.

For regulators and stablecoin issuers globally – especially in jurisdictions considering stablecoin regulatory frameworks like the EU (MiCA) or Switzerland – USDC's compliance model provides a practical benchmark. Its implementation has shown regulators that digital currencies can operate securely and compliantly within decentralized ecosystems if issuer control mechanisms are strategically applied.

In conclusion, USDC's model illustrates a successful approach combining openness, transparency, and robust compliance controls, offering a pragmatic pathway for future stablecoin development and regulation worldwide.

5.2 CryptoFranc (XCHF)

The CryptoFranc (XCHF) was a Swiss Franc–pegged stablecoin launched in late 2018 by Swiss Crypto Tokens AG, a subsidiary of Bitcoin Suisse AG. Designed as a fully compliant "digital CHF," XCHF adhered to Swiss regulatory standards and was classified as a payment token under FINMA's ICO guidelines. Each XCHF token was legally structured as a claim on one Swiss Franc, implemented via an ERC-20 smart contract representing a CHF-denominated bond (with a published prospectus). Importantly, this stablecoin program was discontinued in 2024: Bitcoin Suisse announced in August 2024 that it would cease issuing and redeeming XCHF and wind down the token, aligning the decision with a strategic refocus on core crypto-financial services.

Despite its termination, XCHF remains an informative case study in stablecoin compliance and design, illustrating how a stablecoin can be operated within a strict regulatory framework.

5.2.1 Issuance and Regulatory Compliance

XCHF was issued and redeemed by Swiss Crypto Tokens AG (Bitcoin Suisse's tokenization arm) under defined compliance procedures. Prospective XCHF purchasers had to undergo full Know-Your-Customer (KYC) and Anti-Money-Laundering (AML) verification before tokens could be issued, reflecting strict adherence to Swiss financial regulations.

However, on-chain, XCHF was an ERC-20 token with no transfer restrictions. The tokens "could be traded freely as any Swiss-based bond can be traded peer-to-peer with anyone" on various exchanges and platforms. This effectively meant XCHF did not implement whitelisting; it treated the tokens like traditional bearer instruments and all transactions were subject to the issuer's Token Terms and Swiss law. The assumption were that requiring KYC for redemption (i.e. to cash out the stablecoin) would suffice to mitigate AML risks, similar to how someone might freely trade a bearer bond or cash but would be identified when cashing it in with an institution. XCHF's model was arguably compliant under the standards of the time (2018) – the issuer was a FINMA-supervised financial intermediary (through a self-regulatory organization) and followed AML for its direct interactions. There was no explicit FINMA rule then against intermediate anonymity.

At the time, XCHF's status as a FINMA-designated payment token (rather than a security) helped clarify its regulatory treatment. This classification underscored that the token's sole function was as a payment or value-transfer instrument, with no additional dividend or governance rights. In practice, Bitcoin Suisse AG maintained oversight of XCHF's circulation in line with compliance requirements – as, for example, at redemption, token holders were required to identify themselves and satisfy AML checks before receiving the equivalent CHF payout. These measures ensured that XCHF's issuance and redemption processes were fully compliant with Swiss financial intermediary rules, making it a model for regulatory-conformant stablecoin operation. However, under FINMA's 2024 stance, XCHF's free-transfer model turned to be problematic. FINMA viewed the continuous trading of XCHF among unknown parties as violating the principle that all holders be identified.

5.2.2 Collateralization and Auditing

Every XCHF token was 100% collateralized by Swiss Franc reserves held in custody, ensuring a 1:1 parity with the CHF. Uniquely, the backing assets were reportedly kept as physical Swiss franc banknotes in a secure vault (or "bunker"), rather than in a traditional bank account. This approach provided tangible assurance of solvency and reduced counterparty risk. To bolster transparency, an independent Swiss auditing firm (Grant Thornton Bank Audit Ltd) verified the CHF reserves on a monthly basis, issuing public reports that confirmed

the full backing of all XCHF in circulation. This monthly audit practice was pivotal in establishing trust, as it allowed observers to verify that the token supply never exceeded the actual CHF held in reserve.

Additionally, the XCHF smart contract underwent a comprehensive security audit by Chain Security AG prior to deployment. The audit found no critical vulnerabilities, and any minor issues were addressed before launch. The combination of robust reserve audits and a vetted smart contract exemplified a high standard of technical and financial integrity. During its operation, XCHF was often cited as a best-practice example of a transparent stablecoin: the issuer regularly published attestation reports and legal disclosures, and the token's design included safeguards (such as a bank guarantee on reserves) to protect holders' interests. These features made XCHF one of the most thoroughly audited and securely structured stablecoins in the market during its tenure.

5.2.3 Market Adoption and Legacy

In terms of market use, XCHF was available to both institutional and retail users, though its adoption remained relatively niche. Initially, the primary way to obtain or redeem XCHF was directly through Swiss Crypto Tokens AG's platform, which required an account and compliance onboarding. For convenience, smaller volumes of XCHF could also be traded on several cryptocurrency exchanges. By 2019–2020, XCHF trading pairs were listed on exchanges such as Bitfinex, Ethfinex (DeversiFi), IDEX, and the decentralized exchange Uniswap, providing liquidity for users who did not engage directly with the issuer. This allowed the token to support various use cases in the Swiss "Crypto Valley" ecosystem – for example, as a stable CHF equivalent for tokenized real estate transactions (e.g., on the Blockimmo platform) or other blockchain-based financial services. However, XCHF's overall trading volume and uptake remained modest compared to major global stablecoins. In July 2022, Bitfinex delisted XCHF, citing the cessation of trading support for the token, which hinted at the limited demand in broader markets.

By late 2024, the issuing company decided to end the project. Bitcoin Suisse AG formally announced the discontinuation of XCHF in August 2024, and gradually removed XCHF from circulation over the remainder of that year. The company explained that this move was part of a strategic pivot toward its core offerings in crypto brokerage, custody, and investment products, noting that maintaining a proprietary CHF stablecoin was no longer a priority. XCHF token holders were given a window to redeem their tokens for CHF or convert them into other assets before the final cutoff (end of September 2024 for platform trading, with a subsequent grace period for redemptions). Any remaining unredeemed funds were placed under the custody of a third-party fiduciary (CMP Group AG) for the benefit of token holders, as overseen by Swiss authorities in early 2025.

Although the XCHF token is no longer active, its legacy endures as an important compliance case study. XCHF demonstrated that a fiat-pegged stablecoin could be issued within a rigorous legal framework: it maintained

full reserve transparency, implemented strong investor protections, and operated under Swiss regulatory oversight from inception to wind-down. The project's lifecycle – from launch to orderly shutdown – provides valuable insights for policymakers and practitioners. Even in discontinuation, the XCHF model (with regulated issuance, regular audits, and clear redemption processes) remains a benchmark for comparing other stablecoins' legal and technical architectures.

Future Swiss franc stablecoin initiatives or digital currency projects can draw lessons from XCHF's design and its integration of compliance mechanisms, even as the market evolves beyond this particular token. In summary, CryptoFranc XCHF's rise and termination illustrate both the possibilities and challenges of a fully compliant stablecoin, solidifying its role as a reference point in the discourse on stablecoin regulation and best practices.

5.3 Sygnum Digital CHF (DCHF)

Sygnum Bank, a regulated Swiss digital asset bank, launched its Digital CHF stablecoin in 2020. DCHF is a tokenized representation of Swiss franc deposits held at Sygnum. Because Sygnum is a bank, it can take deposits and the token essentially functions as a claim on the bank (similar to a transferable bank account balance).

5.3.1 Compliance Design

Given Sygnum's regulated status, it implemented DCHF very cautiously. The DCHF smart contract includes role-based controls and a whitelist of addresses in line with regulatory requirements. Only addresses belonging to Sygnum's clients (or authorized partners) are whitelisted. To obtain DCHF, a user must have an account with Sygnum and pass full Swiss bank KYC onboarding. When a client converts CHF to DCHF, the tokens are minted to that client's Ethereum address (which has been whitelisted by Sygnum). If the client wants to transfer DCHF to someone else, that recipient must also be a Sygnum client (or at least have an address whitelisted by Sygnum). The smart contract enforces this by rejecting transfers to any non-whitelisted address. Sygnum thus achieved a fully permissioned stablecoin – essentially a walled garden but using public blockchain infrastructure (the token standard is ERC-20). Additionally, the DCHF contract has a feature to block or "pause" tokens in particular addresses if needed, providing a tool for freezing orders or similar.

5.3.2 Regulatory Outcome

Sygnum's DCHF is fully compliant with FINMA's expectations, as it predates the formal 2024 guidance but was designed per FINMA's 2021 practice (which, as noted, required banks to whitelist stablecoin holders). Indeed, FINMA explicitly cited Sygnum's approach as an example in annual reports. The trade-off is that DCHF's usage is limited – it's primarily used for on-chain settlement among Sygnum and its partners/clients (for example, Sygnum and the e-commerce firm Galaxus piloted a transaction where a customer paid in DCHF

and the merchant instantly redeemed it via Sygnum's system). Important to note, DCHF is not available to the general public without onboarding.

This case shows the strict Swiss model in action: it is feasible, and it meets regulatory approval, but it confines the stablecoin's utility to a closed network of identified users. Sygnum has touted DCHF as a success for bridging crypto and fiat, but its scale remains relatively small compared to open stablecoins like USDC.

5.4 Other Examples

Several other stablecoins illustrate variations of how different compliance mechanisms are implemented.

5.4.1 Tether (USDT)

The largest stablecoin globally is issued by Tether Ltd. While based offshore (with a complex corporate history), Tether follows a compliance approach akin to USDC's. It requires KYC for direct redemption on its platform and cooperates with authorities to freeze addresses: Tether has reportedly frozen over $1 billion in USDT related to hacks and law enforcement requests over the years. Tether does not whitelist all addresses; USDT is widely transacted on numerous blockchains by anyone. Tether's ability to freeze tokens has been used in high-profile cases (e.g. helping recover stolen crypto). This again highlights how major stablecoins balance openness with a backstop of issuer control.

5.4.2 Diem (Libra)

Although never launched, Facebook's proposed Libra (later Diem) stablecoin project had planned a permissioned model initially. As part of seeking Swiss regulatory approval (Libra Association was based in Geneva), the project indicated Libra transfers might be limited to authorized VASPs/wallets for compliance. FINMA's feedback on Libra in 2019 suggested it would be treated strictly under Swiss law, likely needing full AML controls on participants. Diem's fate (wound down in 2022) means it didn't become a reference implementation, but it influenced regulators' thinking about stablecoins and may have spurred FINMA's tougher stance in Switzerland.

5.4.3 XRP and others

Though not a fiat-backed stablecoin, Ripple's XRP (if considered a "payment token") was used in some early pilots for cross-border transfers with KYC at the endpoints. This again followed the principle that blockchain tokens can flow freely while institutions handling them cover AML on their part. This approach is analogous to how tokenized securities are handled: the tokens might circulate, but issuing entities and intermediaries perform KYC when needed (e.g. at issuance or when custody changes in a regulated venue).

5.4.4 USD Stablecoin $USC

A newer project (referenced as "the first Swiss-compliant USD stablecoin") is $USC by Colb Asset SA in Geneva. It reportedly uses a Swiss trust structure: USD is held by a Swiss trust company (Colb SCB USD Issuer Trust) and tokens are issued representing a claim. Under Swiss law, the token represents a debt of the trust to the holder, and they aimed to comply with Swiss AML by whitelisting users and ensuring freeze functionality. This shows ongoing attempts to design stablecoins that meet FINMA's standards while providing useful functionality.

5.5 Deep Dive: CoinVertible (EURCV) – Societe Generale-Forge's Euro Stablecoin

5.5.1 Overview

EUR CoinVertible (EURCV) is an institutional-grade Euro-denominated stablecoin issued by Societe Generale's fintech subsidiary SG-Forge in April 2023. It is fully fiat-collateralized (pegged 1:1 to the Euro) and was designed as a bridge between traditional finance and the digital asset world, combining high transparency and regulatory compliance with the efficiency of public blockchains. Initially launched on Ethereum, SG-Forge has since expanded EURCV to other networks (e.g. Stellar, with plans for Solana) to broaden its use cases in cross-border payments and decentralized finance (DeFi) ecosystems.

As of May 2025, approximately €41.3 million EURCV are in circulation, with daily public updates on supply and reserves to ensure transparency. The coin's name "CoinVertible" reflects its redeemability: holders can redeem EURCV for Euros through SG-Forge or partner platforms (e.g. Bitstamp), subject to compliance checks.

5.5.2 Regulatory Framework and Legal Status

5.5.2.1 EU and French Regulation

EURCV is issued under a robust regulatory framework. In France, it is legally characterized as a "digital asset" (actif numérique) under the 2019 PACTE law and the French Monetary and Financial Code. Societe Generale-Forge is registered with the Autorité des Marchés Financiers (AMF) as a Digital Asset Service Provider and, importantly, has obtained an Electronic Money Institution (EMI) license from the French regulator Autorité de contrôle prudentiel et de résolution (ACPR) in 2024. This EMI license authorizes SG-Forge to issue e-money and essentially allows EURCV to function as electronic money on-chain.

Under the EU's new Markets in Crypto-assets (MiCA) regulation, EURCV is designed to qualify as an "e-money token," meaning it represents electronic money in token form. SG-Forge updated the stablecoin's structure by mid-2024 to fully comply with MiCA's requirements for stablecoins – including capital, investor rights, and

transparency rules – ahead of MiCA's implementation date. Notably, as an e-money token EURCV must be redeemable at par value at all times and is not allowed to restrict coinholder redemption rights.

The ACPR approved SG-Forge's MiCA compliance plan and white paper in October 2024, meaning EURCV was among the first EU stablecoins notified under MiCA's framework. It is not classified as a "significant" e-money token under MiCA (as its scale is below regulatory thresholds), but SG-Forge adheres to similar high standards in reserve management and disclosure. All customer funds backing EURCV are held in segregated, bankruptcy-remote accounts, providing holders with an exclusive claim on those reserve assets even in the event of SG-Forge's insolvency. This legal structure mirrors requirements in traditional e-money and protects coin holders akin to how bank depositors or e-money users are protected.

5.5.2.2 Swiss Relevance

Although EURCV is a Euro stablecoin issued under EU/French law, its regulatory model holds insights for Switzerland. Switzerland currently lacks a specific "e-money token" category; a Swiss franc stablecoin is generally treated as a form of deposit or a digital representation of funds. The SG-Forge approach – obtaining an e-money issuer license and providing a regulator-approved white paper – illustrates one path to issuing a fiat-backed stablecoin within a clear regulatory perimeter. By contrast, in Switzerland a non-bank issuer of a CHF-pegged stablecoin might need to seek a fintech license or bank license to accept public CHF funds, or otherwise structure the token as a security. The French/EMI model highlights how a mid-sized financial institution can issue a stablecoin under supervisory oversight without a full banking license, a concept that could inform Swiss discussions on regulating stablecoin issuers outside the traditional banking sector. Additionally, SG-Forge's compliance with MiCA demonstrates how comprehensive stablecoin regulation can foster greater trust and adoption – an outcome Swiss policymakers may consider as the EU framework comes into effect.

5.5.3 AML/KYC and Compliance Measures

5.5.3.1 Off-Chain Compliance (KYC/AML)

From inception, EURCV was targeted at institutional and accredited participants, and SG-Forge integrated strict compliance checks into the issuance and redemption process. Initially, only whitelisted SG-Forge clients (who underwent full KYC onboarding) could hold or transact EURCV, effectively making it a permissioned stablecoin in its early phase. This whitelist approach ensured that every wallet holding EURCV was associated with an identified customer, simplifying anti-money-laundering monitoring.

In late 2023, SG-Forge upgraded the smart contract for "free transferability" as part of MiCA readiness, removing the whitelist restriction to allow broader use of EURCV on public blockchains. However, compliance

remains stringent: even though any Ethereum address can now technically receive EURCV, only verified customers can mint new EURCV or redeem it for Euros. SG-Forge and its partners (like Bitstamp for redemption) require standard KYC/AML vetting before converting fiat to EURCV or vice versa. This means EURCV can circulate freely on-chain between users (enabling use in DeFi or peer-to-peer transfers), while entry and exit points to the fiat system are gated by compliance controls – a model similar to other major stablecoins.

SG-Forge employs additional measures to uphold financial crime compliance. The firm's technical platform is built on the open-source CAST framework ("Compliant Architecture for Security Tokens"), which facilitates integration of compliance rules (e.g. investor whitelists, transfer restrictions) into blockchain assets. Through CAST or similar tooling, SG-Forge can monitor EURCV transactions in real time and flag suspicious activity. Unusual on-chain movements are subject to investigation under SG-Forge's AML policies, and the firm has stated it "monitors EURCV circulation" closely. In practice, SG-Forge likely leverages blockchain analytics and off-chain data to track illicit use. The post-MiCA free transferability necessitates a shift from a preventive whitelist approach to a detect-and-react approach: rather than stopping all unvetted transfers, SG-Forge permits open transfers but can blacklist addresses involved in illicit activities (as discussed in more detail below) and will refuse redemption to holders who violate compliance rules.

This hybrid model attempts to balance open usability (a key requirement under MiCA's vision of "open" stablecoins) with controlled risk and reflects a broader industry trend among regulated stablecoins.

5.5.3.2 On-Chain Controls (Whitelist, Blacklist, Freezing)

The EURCV smart contract includes administrative functions that enable SG-Forge to enforce certain controls on-chain. According to the EURCV White Paper, SG-Forge reserves the right to blacklist specific blockchain addresses that it determines (at its discretion) are associated with sanctioned actors, money laundering, or other illegal activities. If a blacklisted address is detected, the issuer can freeze any EURCV tokens held at that address or even that have transited through it. Freezing essentially renders the tokens non-transferable, preventing further movement.

In extreme cases (e.g. a law enforcement order or court injunction), SG-Forge may even confiscate or nullify the stablecoins in question and might be required to surrender the equivalent fiat collateral to authorities. These control mechanisms are analogous to those used by other regulated stablecoin issuers – for instance, Circle's USDC contract allows blacklisting of addresses and freezing of USD Coin balances, a power that was notably used to freeze USDC in OFAC-sanctioned Tornado Cash wallets in 2022. In the case of EURCV, such powers have not been publicly exercised to date, but their existence provides confidence to regulators that the issuer can intervene if the stablecoin were implicated in illicit finance or if required by law.

It is worth noting that the contract was audited for security and compliance by external auditors (e.g. Hacken audited the EURCV Ethereum smart contract in June 2024). This creates a high level of confidence that the administrative functions (minting, burning, blacklisting, etc.) operate as intended and that there are no apparent vulnerabilities that could be exploited to bypass controls or alter balances.

Early-stage whitelisting ensured only vetted users held EURCV, and now blacklist/freeze tools provide a backstop for compliance in a freely transferable environment. This two-layer approach – off-chain KYC at fiat gateways and on-chain enforcement capabilities – exemplifies how a regulated stablecoin can maintain AML standards without sacrificing the advantages of public blockchain infrastructure. Swiss regulators and stablecoin projects are closely studying such designs, as they address one of the key challenges: reconciling financial integrity requirements with open blockchain usage.

5.5.4 Reserve Management and Transparency

An important characteristic of EURCV is its conservative reserve management and high transparency, aligning with both regulatory obligations and industry best practices. Every EURCV token in circulation is 100% backed by an equivalent amount of Euro held in segregated bank accounts. SG-Forge holds the reserves with reputable financial institutions (likely including Société Générale group entities or custodial banks), and these funds are ring-fenced from SG-Forge's own assets. In practice, this means that even if SG-Forge were to face bankruptcy, EURCV holders have a priority claim on the reserve funds, and other creditors cannot tap those assets. This setup meets MiCA's mandates for stablecoin issuers to safeguard reserve assets and mirrors the EU E-Money Directive's protections for electronic money float.

SG-Forge provides daily public reporting on the total EURCV in circulation and the corresponding collateral value. On its website, the firm updates metrics each business day, showing the outstanding token supply and confirming a 100% collateralization ratio, along with the total Euros held as collateral. This frequency of disclosure goes beyond many other stablecoin issuers which often publish monthly attestations. Additionally, SG-Forge has published a comprehensive White Paper (updated to version 2.1 in October 2024) detailing the stablecoin's legal terms, risk factors, technical design, and reserve management approach. The White Paper and accompanying documents serve as the required disclosure under MiCA and are lodged with the French regulator. While not a public audit, these documents, combined with periodic audits of SG-Forge as an entity, contribute to transparency. For further assurance, SG-Forge could engage an external auditor or provide on-chain proofs of reserves in the future, but at minimum it follows the compliance of an EMI (which includes audits of safeguarding controls).

In the context of Swiss stablecoins, the EURCV's approach to reserve management underscores the importance of asset segregation and disclosure. FINMA has similarly indicated that stablecoin issuers must

fully back tokens with high-quality, liquid assets and preferably hold them with minimal risk. For example, Sygnum's DCHF stablecoin is fully backed by equivalent CHF deposits held at the Swiss National Bank – an even more risk-free reserve setup. While SG-Forge uses commercial bank accounts for EURCV's reserves (since only banks can access central bank deposits in Euros), it mitigates risk by only using secure custodians and holding a conservative asset mix (likely only cash or overnight sweeps). No interest or yield is generated on the reserves (as is typical for stablecoins), and SG-Forge does not engage in fractional reserve practices. This conservative stance aligns with the "stable" in stablecoin, prioritizing parity and redemption at all times over any potential investment income from the float.

5.5.5 Comparison to Other Regulated Stablecoins

5.5.5.1 EURCV vs. USD Coin (USDC)

EURCV and USDC share a similar ethos of regulatory compliance and full backing, though they operate under different jurisdictions and scale. USDC (issued by Circle and Coinbase via the Centre consortium) is a U.S. dollar stablecoin that has become one of the largest globally. Like EURCV, USDC is fully reserved (with cash and short-term treasuries) and provides frequent attestations of its collateral. Both stablecoins employ on-chain freeze controls to address illicit use – in fact, USDC's issuer has previously blacklisted addresses linked to sanctioned activities, demonstrating a comparable commitment to compliance as EURCV's blacklisting policy.

A key difference is regulatory status: Circle is regulated as a money services business and has obtained state-level licenses in the U.S., but there is not yet a unified federal stablecoin framework. In contrast, SG-Forge operates under a specific EU regulatory regime (MiCA/EMI). Another difference is market reach: USDC is widely used in global crypto markets and DeFi applications, with a circulation in the tens of billions of USD. EURCV, being newer and Euro-denominated, has a more modest supply (~€40 million) and is in an adoption phase. However, SG-Forge is positioning EURCV as a European alternative to USD-backed stablecoins, and its regulatory pedigree may attract institutions that require a fully compliant Euro token. Notably, both USDC and EURCV have embraced multichain strategies – USDC exists on multiple blockchains (Ethereum, Algorand, Solana, etc.), and EURCV is now on Ethereum and Stellar, with plans for further chains to increase their accessibility and use cases.

5.5.5.2 EURCV vs. Sygnum Digital CHF (DCHF)

DCHF is a Swiss franc stablecoin issued by Sygnum Bank, and it provides an instructive comparison as a fully regulated bank-issued stablecoin in Switzerland. Like EURCV, DCHF is 1:1 fiat-backed and aimed at institutional usage. Sygnum, being a licensed Swiss bank, holds an equivalent amount of CHF for every DCHF token in a sight deposit at the Swiss National Bank – arguably the safest form of collateral possible. This means

DCHF represents a direct digital claim on central bank money, whereas EURCV represents a claim on commercial bank-held money (albeit safeguarded).

In terms of accessibility, DCHF has so far been used as a settlement token within Sygnum's ecosystem (for instant settlement of tokenized securities trades, etc.) and by select partners. It was the first stablecoin issued by a regulated Swiss bank, underscoring Switzerland's innovative approach, but it remains somewhat closed-loop. Only Sygnum clients (who undergo full KYC) can mint or redeem DCHF, and transfers likely occur among permissioned addresses or approved platforms. This contrasts with EURCV's post-MiCA open transferability, where anyone can hold and transfer it on public networks.

In terms of on-chain controls, DCHF's smart contract, much like EURCV's, includes features for pausing, freezing, and even confiscating tokens if required by law or court order. This reflects a common design philosophy: regulated institutions build in the capability to intervene on-chain, even if used sparingly.

For Swiss regulators and market participants, DCHF exemplifies the "bank-issued stablecoin" model (sometimes called a deposit token when issued by a bank). EURCV shows a slightly different path – a non-bank subsidiary with an e-money license – but both achieve similar outcomes in collateral certainty and compliance. One practical difference is scale and usage: EURCV, through partnerships (Bitstamp, Wintermute, etc.), is gearing up for broader trading and DeFi use, whereas DCHF has been focused on institutional settlement and even experimented with e-commerce payments in a limited context. Going forward, if Swiss banks or Fintechs issue CHF stablecoins for public use, they may take cues from EURCV's approach to balancing openness with oversight.

5.5.5.3 EURCV vs. CryptoFranc (XCHF)

XCHF provides a case study of a Swiss stablecoin initiated outside the banking system. Launched in 2018 by Swiss Crypto Tokens AG (an affiliate of Bitcoin Suisse), XCHF was an ERC-20 token pegged to the Swiss Franc and fully backed by CHF deposits held by the issuer. It was structured legally as a form of bond or structured token, and Swiss authorities treated it as a payment token under the FINMA ICO guidelines rather than as a deposit or security. This regulatory characterization meant XCHF could circulate without a banking license, but the issuer still voluntarily maintained 100% reserves and offered redemption.

Compliance was ensured off-chain: holders had to go through Bitcoin Suisse's KYC/AML process to redeem XCHF for francs, and the terms of the token allowed the company to refuse service to sanctioned persons. However, XCHF did not implement strict on-chain controls like whitelisting or automated freezes – it operated more like a traditional cryptocurrency token, relying on the issuer's off-chain enforcement of compliance during redemption.

While XCHF proved that a non-bank entity could issue a stablecoin under Swiss law, it saw limited adoption (peaking at a few hundred thousand CHF in circulation) and faced increasing operational and regulatory hurdles. In mid-2024, Bitcoin Suisse announced the discontinuation of XCHF and ceased issuing or redeeming tokens. By early 2025, the remaining outstanding XCHF were in the process of being redeemed or transferred to a custodian for wind-down.

The XCHF experience highlights the challenges for a stablecoin without a robust regulatory framework: despite being fully collateralized and compliant with basic AML rules, it lacked the explicit supervisory oversight that institutions like SG-Forge or Sygnum have. For the Swiss stablecoin discussion, XCHF's rise and closure emphasize the importance of clear regulatory support and possibly the need for a dedicated category (since XCHF was essentially an improvisation around existing laws). It also suggests that trust (or the lack thereof) can be a limiting factor – market participants may prefer stablecoins issued by well-regulated institutions (banks or licensed e-money issuers) over those by independent crypto firms, especially for larger scale use.

5.5.5.4 Conclusion of Comparisons of EURCV to Other Regulated Stablecoins

CoinVertible (EURCV) stands alongside USDC, DCHF, and (formerly) XCHF as part of a class of fully-reserved, fiat-pegged stablecoins with regulatory oversight. All share the goal of stability and trust, but their approaches differ: USDC and EURCV are open-market stablecoins accessible to broad users (with EURCV's openness only recently achieved via MiCA compliance), whereas DCHF (bank-issued) and the now-defunct XCHF took a more closed or niche approach. From a compliance perspective, EURCV and USDC implement on-chain freezes/blacklists proactively, Sygnum's DCHF enforces compliance through banking controls and could intervene on-chain if needed, and XCHF relied on off-chain measures and ultimately bowed out under regulatory pressure.

These examples collectively inform regulators and industry in Switzerland – demonstrating that while technology allows a spectrum from permissioned to permissionless designs, the market seems to favor those stablecoins that achieve high regulatory assurance (and integration with the traditional financial system) alongside the technical advantages of crypto. Swiss authorities, in evaluating stablecoin frameworks, can observe that standards like 100% reserve backing, daily transparency reporting, redemption at par, regulatory licensing, and embedded compliance controls are becoming the norm for any stablecoin intended for mainstream use.

5.5.6 Implications for Swiss Stablecoin Regulation and Design

The case of CoinVertible (EURCV) offers several learnings for Switzerland's ongoing discourse on digital franc stablecoins and potential regulatory regimes.

5.5.6.1 Clear Regulatory Status

SG-Forge's ability to launch EURCV hinged on fitting it into an existing legal category (e-money) and obtaining a license. This suggests that Switzerland may need to either utilize existing categories (such as banking or fintech licenses) or develop a new framework to give stablecoin issuers legal certainty. The EU's MiCA approach – explicitly defining e-money tokens and requiring authorization and disclosure – could serve as a model. Swiss regulators might consider formal guidelines or a regime for "stable value tokens" to clarify their treatment (as FINMA previously did for ICO tokens). The absence of a clear path was one factor in XCHF's discontinuation, whereas SG-Forge's regulated status enabled EURCV's growth.

5.5.6.2 Issuer Qualification – Banks vs. Non-Banks

EURCV demonstrates that a non-bank financial entity can successfully issue a stablecoin with the right license and oversight. In Switzerland, the prevailing view has been that a CHF-backed stablecoin redeemable from a wide audience likely constitutes a public deposit (hence requiring a banking license unless an exemption applies). The SG-Forge model provides a middle ground: a lightly licensed entity (EMI) under central bank and prudential supervision can issue stablecoins without being a full bank.

Swiss authorities could explore an analog: for instance, expanding the scope of the fintech license (which currently allows accepting public deposits up to CHF 100 million) to explicitly cover stablecoin issuance, coupled with safeguard requirements. Alternatively, encouraging existing licensed banks to issue stablecoins (as Sygnum did) is the other route. The Swiss National Bank and banking industry have recently discussed "deposit tokens" – tokenized commercial bank money. EURCV is essentially SocGen's version of a deposit token (backed by SocGen's e-money float). This implies that Swiss banks could follow suit, and regulators should be prepared to supervise such activities, ensuring no gaps in consumer protection or financial stability.

5.5.6.3 Compliance Architecture

EURCV's evolution from a permissioned, KYC-only token to an open but controllable token underscores technological solutions to AML compliance. Swiss implementation can mirror this by mandating that stablecoin issuers maintain the capability to freeze or disable tokens linked to illicit use, and to screen transactions as needed. FINMA's guidance for virtual asset service providers already requires transaction monitoring and sanctions screening; extending such expectations to any Swiss franc stablecoin issuer would be prudent. The CAST framework and Sygnum's smart contract suite show that compliance features can be coded into the token contract.

Swiss stablecoin projects should incorporate such programmable compliance from the outset, to satisfy regulators that even on a public blockchain, illicit activity can be addressed. This will be especially crucial if a CHF stablecoin is to be used in open systems or DeFi, where traditional off-chain controls are harder to apply.

5.5.6.4 Segregation and Stability Mechanisms

Another takeaway is the importance of legally segregating reserve assets and having clear recovery/redemption plans. MiCA requires issuers like SG-Forge to maintain recovery plans and redemption arrangements to handle crises. Swiss regulators could similarly require that any stablecoin issuer must segregate reserves (e.g., hold CHF funds in a fiduciary capacity for token holders) and have wind-down plans (so holders aren't stuck if the issuer exits the business). The XCHF wind-down in 2024 was handled by appointing a third-party custodian to return funds, which was an ad hoc solution. A regulated approach would bake in these protections in advance. Additionally, stability mechanisms like 1:1 redemption at par at all times should be a strict requirement – SG-Forge and Sygnum both uphold this, which sustains the price peg and user confidence. Any deviation (like limiting redemptions or holding risky reserve assets) would undermine the "stable" aspect and likely be unacceptable to Swiss authorities (as it is under MiCA).

5.5.6.5 Integration with Traditional Finance

SG-Forge's initiative also shows the value of integrating stablecoins with existing financial market infrastructure. EURCV's use cases include facilitating on-chain settlement for securities tokens and enabling faster cross-border payments. In the Swiss context, a CHF stablecoin could similarly serve as a settlement layer on platforms like SDX (Six Digital Exchange) or for interbank transactions, complementing or advancing projects like SDX's own CHF settlement coin or the SNB's wholesale CBDC experiments. If Swiss regulators see a stablecoin fulfilling a public good (e.g. improving settlement efficiency), they might be more inclined to support its development. The fact that a major banking group (Societe Generale) is behind EURCV lent it credibility; in Switzerland, any successful CHF stablecoin might likewise involve established financial institutions to gain traction. Swiss banks could collaborate on a common CHF stablecoin standard (as suggested by the Swiss Bankers Association's 2023 proposal for a joint deposit token), taking cues from EURCV's technical and governance design.

In conclusion, CoinVertible (EURCV) exemplifies a next-generation regulated stablecoin that marries the trustworthiness of traditional finance with the openness of crypto networks. Its regulatory framework (EMI license + MiCA compliance), rigorous KYC/AML controls, on-chain oversight features, and commitment to transparency set a high bar for stablecoin projects. For Switzerland, which prides itself on strong financial regulation and innovation, EURCV provides a concrete reference model. Swiss regulators may not copy the EU approach wholesale, but the core principles observed here – full backing, redeemability, licensing, supervision, and technological controls – are likely to underpin any Swiss-endorsed stablecoin as well. As the landscape evolves, the experience of EURCV and its peers (USDC, DCHF, etc.) will continue to inform the best practices and regulatory standards for stablecoins in Switzerland and globally.

5.6 Summary of Case Studies

The case studies analyzed reveal a clear spectrum of compliance and regulatory alignment among stablecoins, highlighting distinct approaches across different jurisdictions and design philosophies. Open-market stablecoins such as USDC and USDT have achieved global scale by prioritizing broad accessibility, only intervening selectively through blacklisting and cooperating with authorities to manage illicit activities. By contrast, regulated stablecoins like the EU-based EUR CoinVertible (EURCV) exemplify stringent oversight, embedding compliance directly into the token's infrastructure through on-chain mechanisms like issuer-managed pause, freeze, and blacklist controls. EURCV, issued by a licensed institution under the MiCA e-money token framework, ensures transparency and security, with reserves fully segregated and redeemable at par, thus aligning with robust consumer protection and financial integrity standards.

Swiss stablecoin initiatives, responding to stringent national AML/KYC regulations, have historically adopted narrower models: tokens like DCHF maintained a closed-loop, fully KYC-compliant environment, while projects like XCHF utilized securities-like structures to mitigate regulatory burdens. However, given the current trajectory set by FINMA, future Swiss franc stablecoins may increasingly need to adopt the comprehensive whitelisting model exemplified by Sygnum's DCHF unless regulatory adjustments explicitly allow alternatives. Globally, hybrid and protocol-level compliance solutions are emerging, with issuers exploring smart contracts that autonomously enforce compliance thresholds or integrate identity verification protocols directly on-chain.

Ultimately, these diverse regulatory and operational frameworks demonstrate an ongoing industry effort to balance innovation and regulatory compliance. Lessons from EURCV, DCHF, and other models illustrate how robust regulation can enhance credibility, foster integration with traditional finance, and potentially set industry benchmarks. As technology and legal frameworks continue to evolve, stablecoin issuers must navigate carefully, managing the trade-offs between openness, efficiency, and stringent oversight to achieve sustainable, compliant growth.

6. Swiss Law: Freezing, Blocking and Investor Rights

An important aspect of stablecoin regulation is understanding the rights of holders and the powers of issuers or authorities to block or seize tokens. Under Swiss law, several layers of legal authority come into play when a stablecoin is frozen or blocked – whether by the issuer's decision or by government order. This section clarifies the civil law implications of such actions, as well as the criminal procedure for seizure (Art. 263 of the Swiss Criminal Procedure Code).

6.1 Holder Rights and Contractual Terms

A stablecoin issued by a centralized entity typically gives the holder a contractual claim against the issuer (for redemption of the underlying asset, e.g. 1 CHF or 1 USD per token) or represents some property interest. For example, holding XCHF is holding a bond; holding DCHF is effectively a claim on Sygnum Bank's deposit. Swiss civil law (the Code of Obligations) mandates that contractual claims be honored according to their terms. If a holder meets the conditions for redemption (e.g. properly identified and not engaged in crime), they have a right to redeem their stablecoins for cash. If an issuer were to unilaterally block a holder's access or refuse redemption without legal justification, it could constitute a breach of contract or even an unlawful appropriation. However, in practice, issuers protect themselves by incorporating compliance clauses into user agreements. Stablecoin terms of service often stipulate that the issuer can deny service, freeze assets, or delay redemption if needed to comply with laws (such as AML regulations or sanctions) or if suspicious activity is detected. By agreeing to use the stablecoin (or by the contractual framework of purchase/redemption), holders consent to these conditions. Thus, withdrawal/redemption rights are not absolute – they are subject to compliance with law and the platform's rules.

6.2 Swiss Civil Law

Under Swiss civil law, money held in a bank account gives the customer the right to withdraw at any time, but banks may freeze accounts when required by law (e.g. AMLA's duty to freeze after a suspicious activity report). Similarly, a stablecoin issuer can invoke legal obligations as a defense for not executing a redemption immediately. If a holder is blocked because they are on a sanctions list or failed to provide information, the issuer is arguably excused from performance until the issue is resolved. Furthermore, if the stablecoin is structured as a security, the rights of the holder are defined by the security's terms. As an example, in XCHF's case, the bond terms likely allow suspension of redemption in extraordinary cases (much like how a company might defer a bond payment if legally compelled). The principle "no one should profit from illegal acts" also plays a role – a holder engaged in money laundering or sanctions evasion cannot expect the issuer to honor the claim without question. However, if an issuer freezes a law-abiding customer's funds erroneously, that customer could have legal remedies. They might demand performance (redemption) or potentially claim damages if they incurred loss due to an improper freeze.

6.3 Property Law Considerations

Swiss law traditionally did not recognize digital tokens as a category of property, but the 2021 DLT law amendments introduced the concept of "register value rights" ("Registerwertrechte") that can be property-like. If a stablecoin is issued as a register value right (a ledger-based security), the holder is recognized as having a property-like right in the token vis-à-vis the issuer. Freezing or deleting such tokens could be seen as interfering with the holder's property. Even if tokens are not yet fully recognized as property chattels, Swiss courts have treated crypto assets as assets that can be owned and stolen. Freezing someone's stablecoin could be seen analogously to freezing their bank account or other asset: allowable only under law. From the civil law perspective, ownership doesn't officially transfer when something is frozen – the person remains the owner/creditor, but their ability to dispose is (temporarily) suspended. This is generally acceptable if done under legal authority or contract, but not if done arbitrarily.

6.4 Issuer Freezing vs. Authority Freezing

It is useful to differentiate a freeze initiated by the issuer (contractual/voluntary) and a freeze mandated by authorities.

6.4.1 Issuer-Initiated Blocking

This might occur if the issuer detects suspicious activity (e.g. a hack or an AML red flag) and proactively freezes tokens to prevent harm or legal violations. Under Swiss AMLA, if a financial intermediary (issuer) suspects a connection to criminal money or terrorist financing, they must file a report and freeze the assets for up to 5 working days (while authorities decide whether to seize). The law gives them a safe harbor to do so – they are protected from liability for freezing during that period if done pursuant to an AML report. Contractually, issuers also reserve broad rights to freeze to comply with regulations. So an issuer's freeze in line with AML duties is legally justified. If an issuer froze assets without a clear legal or contractual basis (say, due to a mere internal error or dispute), they could face breach of contract claims. In practice, issuers are risk-averse and will freeze only for compliance reasons, not whims.

6.4.2 Authority-Mandated Seizure

Swiss authorities can compel freez or seizures through legal orders. Under Art. 263 of the Swiss Criminal Procedure Code (StPO), prosecutors or courts can seize assets that may be evidence or subject to forfeiture (e.g. proceeds of crime). This provision provides the legal basis to seize cryptocurrency or stablecoins during investigations. In a traditional bank scenario, authorities send the bank a seizure order and the bank freezes the suspect's account. For stablecoins, similarly, if the tokens are held via an issuer or controlled environment, authorities can order the issuer to freeze the relevant tokens or refuse redemption. Art. 263 StPO allows for seizing "objects or assets" – and crypto-assets, despite being data, can be seized either by taking control of

private keys or by instructing an intermediary who has influence over them. If a stablecoin is on a public blockchain, authorities have used methods like obtaining the private key (through cooperating witnesses or suspects) or, more straightforwardly, asking the issuer to blacklist the address (thus immobilizing those tokens). Various legal analysis of crypto seizures suggest that if crypto is held with a service provider, the authorities seize it by treating it as a claim against that provider – i.e., they instruct the provider not to honor the claim to the customer (prevent payout). This is akin to telling a stablecoin issuer "do not redeem or transfer these specific tokens for the suspect." Importantly, under Art. 263, the ownership doesn't transfer to the state at seizure stage; it's a temporary custody measure. If the case concludes and the assets are legitimate, they must be released back to the owner. If deemed illegal proceeds, then a court can order forfeiture (permanent confiscation) later.

For stablecoin users, this means that Swiss authorities have clear power to freeze or seize stablecoins tied to criminal cases. Indeed, in international cooperation, there have been instances of Swiss custodians asked to freeze crypto assets. A stablecoin issuer in Switzerland must comply with such orders or potentially face legal consequences themselves.

6.5 Interaction of Civil and Criminal Law

Suppose an issuer freezes a user's stablecoins due to an authority's seizure order under Art. 263 StPO. The user might claim a right to redeem or transfer, but the criminal law order supersedes that: compliance with the order is a lawful excuse for the issuer to refuse the user's request. The user would have to contest the freeze through legal channels (e.g. argue to unfreeze if they believe it was unwarranted). Swiss law provides procedures for affected parties to challenge seizures in court, ensuring due process. Meanwhile, the issuer is effectively shielded from liability by acting under official order.

Another scenario is sanctions blocking: If the Swiss government (through SECO) imposes sanctions on certain individuals, any assets of those individuals, including stablecoins, must be frozen. This isn't Art. 263 (criminal code) but rather the Embargo Act and related ordinances. Still, an issuer freezing under sanctions law is legally mandated. Civilly, the sanctioned person loses the right to use or redeem assets until sanctions are lifted.

In all, Swiss civil law recognizes the primacy of legal compliance when it comes to asset freezes. The concepts of good faith and contract performance allow that if performance (redemption/transfer) would violate law, the obligation is suspended. However, if an issuer oversteps – e.g., freezes without proper cause – it could face civil liability. This tension pushes issuers to have clear policies and documentation. Many include an arbitration clause or Swiss forum selection for disputes with users, but one could imagine a user suing a Swiss issuer for wrongful blocking. They would have to prove the issuer had no valid justification.

6.6 Investor Protection and Withdrawal Rights

From a policy perspective, a stablecoin holder should know under what conditions they can redeem and when those rights might be curtailed. FINMA's stablecoin guidance also touches on consumer protection – requiring clear disclosures if redemption could ever be halted (for example, some stablecoins might temporarily suspend redemption in extreme market conditions or if reserves are questionable; FINMA would likely not approve that except perhaps in a regulated prospectus). In the case of Swiss stablecoins with bank guarantees (to avoid banking license), one condition FINMA listed is that customers must be able to call the guarantee rapidly. That implies the user's right to get their money back is fundamental. If an issuer freezes someone not for legal reasons but due to insolvency or other failure, the user could call on the bank guarantee to get paid from the guarantor. Thus, even with freezes, the holder's ultimate claim is intended to be protected (at least against commercial risks).

6.7 Summary of legal situation reg. blocking or freezing in Switzerland

Under Swiss law, stablecoin issuers have the ability – and indeed the obligation – to block or freeze tokens in certain scenarios:

- To comply with AML obligations (temporary freeze during a suspicious activity report),
- To comply with sanctions requirements (blocking designated persons),
- To follow a criminal seizure order under Art. 263 StPO,
- Or as otherwise permitted by their contract (e.g. terms allowing freeze if user breaches terms or if required by law).

Holders, on the other hand, retain their contractual rights but with the caveat that those rights can be lawfully suspended when law or contract allows. They do not have an absolute right to transfer or redeem at all times in all circumstances. However, they do have the right to due process – if a freeze is due to a mistake or if they are not actually the target of enforcement, they can seek to have it lifted. The balance struck is one of ensuring compliance without outright confiscation unless warranted.

From a reputational viewpoint, stablecoin issuers must handle freezes carefully to maintain trust. Every freeze is effectively an interference in what users think of as "their money." Swiss civil law, by emphasizing contractual clarity and legal basis, ensures that such power is not unchecked. As stablecoins grow, these legal safeguards will be tested and likely refined, but as of 2025, the framework in Switzerland gives issuers robust authority to freeze assets for compliance, while also delineating the pathways for authorities to seize assets lawfully and for holders to challenge or redeem when appropriate.

7. Overall Conclusion

Switzerland's regulatory stance on stablecoins embodies the country's broader fintech strategy: encouraging innovation while rigorously safeguarding financial stability and integrity. FINMA's latest Guidance 06/2024 clearly illustrates that Swiss stablecoin issuers currently face some of the world's most stringent AML/KYC compliance requirements. Notably, the near-mandatory practice of whitelisting stablecoin holders to preclude anonymous transfers significantly diverges from regulatory approaches in other major financial centers such as the U.S., the UK, the EU, and Singapore. In these jurisdictions, regulators have largely leveraged existing AML frameworks, applying targeted enforcement and on-chain interventions rather than requiring comprehensive identity checks on every participant in token transactions.

The comparative analysis provided throughout this document highlights a spectrum of stablecoin regulatory approaches, underscored by examples like USDC and EUR CoinVertible (EURCV). USDC's "open-but-supervised" model, with its combination of off-chain KYC/KYB protocols and selective on-chain blacklisting, illustrates a globally accepted, flexible approach that satisfies regulatory scrutiny without severely restricting usability. EURCV, under the EU's comprehensive MiCA regulatory framework, takes a different approach, embedding rigorous compliance controls directly into its issuance structure and on-chain mechanisms, thereby aligning closely with traditional financial standards. The successful launch and adoption of EURCV demonstrate that clear and explicit regulatory frameworks, such as MiCA, can significantly boost market confidence, facilitating sustainable growth and cross-border digital currency interoperability.

In contrast, Swiss stablecoin projects historically followed narrower pathways due to stricter regulatory expectations. Tokens like the discontinued XCHF attempted compliance through security-like structuring, while Sygnum Bank's DCHF represents a fully regulated, whitelisted stablecoin model confined primarily within institutional environments. The discontinuation of XCHF in 2024 underlines the operational challenges posed by evolving compliance demands and highlights the practical difficulties of sustaining stablecoins outside clearly defined regulatory perimeters.

Looking forward, there is a growing consensus among Swiss legal and industry experts that the current regulatory environment, though robust, may be too restrictive to be economically viable and competitive internationally. Consequently, there is significant momentum toward refining existing regulations, potentially creating a tailored regime for stablecoins. Drawing inspiration from frameworks like MiCA, Swiss authorities might introduce categories specifically addressing stablecoin issuance and incorporate innovative compliance mechanisms like on-chain identity protocols, monitoring, zero-knowledge proofs, or selective blacklisting, providing a balanced, nuanced regulatory landscape. Such adjustments would help position Switzerland strategically between stringent oversight and technological neutrality, preserving both financial security and market innovation.

Practically, stablecoin issuers in Switzerland currently must partner closely with licensed financial institutions or maintain strict token transfer restrictions to fulfill regulatory expectations. Early engagement with FINMA remains crucial for clarifying compliance expectations. Moreover, Swiss regulators must recognize the ongoing usage of internationally issued stablecoins (e.g., USDC) by Swiss residents and businesses, acknowledging potential exposure risks associated with more open foreign stablecoins. This dynamic suggests a practical incentive for Swiss authorities to adapt the domestic regulatory framework, ensuring it remains competitive, secure, and aligned with global practices rather than driving innovation abroad.

Ultimately, Swiss stablecoin regulation stands at a pivotal juncture in 2025. The detailed analysis in this document emphasizes that Switzerland's foundational legal mechanisms – such as AMLA, Banking Act, and FINMA's directives – offer strong regulatory tools but currently impose comparatively high compliance barriers. Regulatory clarity exemplified by the EU's MiCA framework and practical cases such as EURCV illustrate paths toward a balanced regime that promotes innovation, compliance, and stability simultaneously. The evolving Swiss landscape presents regulators and industry participants with critical choices: either maintaining rigorous, possibly restrictive oversight or embracing a more flexible, yet secure regulatory approach informed by global best practices. Given Switzerland's commitment to high financial standards and technological leadership, ongoing regulatory dialogues and international collaboration will likely refine its stablecoin approach, balancing robust oversight with necessary innovation to facilitate sustainable, compliant, and competitive growth in the stablecoin ecosystem.

8. References

- Anti-Money Laundering Act (AMLA), SR 955.0. (2023). Federal Act on Combating Money Laundering and Terrorist Financing. Available at: https://fedlex.data.admin.ch/eli/cc/1998/892_892_892/en

- Bitcoin Suisse AG. (2025). CryptoFranc (XCHF) - the Swiss Franc Stablecoin. Available at: https://www.bitcoinsuisse.com/cryptofranc

- Centre Consortium. (2022). USDC Blacklisting Policy. Available at: https://www.centre.io/usdc-blacklisting-policy

- Chainalysis. (2022). Understanding Tornado Cash, Its Sanctions Implications, and Key Compliance Questions. Available at: https://www.chainalysis.com/blog/tornado-cash-sanctions-challenges/

- Financial Action Task Force (FATF). (2019). Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. FATF/OECD. Available at: https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf

- Financial Conduct Authority (FCA). (2023). Discussion Paper DP23/4: Regulatory Framework for Stablecoins. FCA Publications. Available at: https://www.fca.org.uk/publications/discussion-papers/dp23-4-regulating-cryptoassets-phase-1-stablecoins

- Financial Crimes Enforcement Network (FinCEN). (2019). Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies (CVC). Available at: https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf

- FINMA. (2021). Guidelines on ICOs: Initial Coin Offerings. Available at: https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/

- FINMA. (2022). Annual Report 2021. Swiss Financial Market Supervisory Authority. Available at: https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/finma-publikationen/geschaeftsbericht/20220405-finma_jahresbericht_2021.pdf

- FINMA. (2024). Guidance 06/2024 – Stablecoins: Risks and Challenges for Issuers of Stablecoins and Banks Providing Guarantees. Swiss Financial Market Supervisory Authority. Available at: https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/04-dokumentation/finma-aufsichtsmitteilungen/20240726-finma-aufsichtsmitteilung-06-2024.pdf

- Homburger AG. (2024). FINMA Publishes Guidance on Stablecoins. Homburger Bulletin. Available at: https://www.homburger.ch/en/insights/finma-publishes-guidance-on-stablecoins

- Kuhn, H. (2024). FINMA Publishes Guidance 06/2024 on Stablecoins – Initial Assessment. Lawside. Available at: https://lawside.ch/finma-publishes-guidance-06-2024-on-stablecoins/

- LALIVE. (2021). International Fraud & Asset Tracing: Enforcement against crypto-assets in Switzerland. Retrieved from Available at: https://www.lalive.law/wp-content/uploads/2024/03/International-Fraud-and-Asset-Tracing-2021-Switzerland-FINAL.pdf

- Monetary Authority of Singapore (MAS). (2020). Notice PSN02 – Prevention of Money Laundering and Countering the Financing of Terrorism – Digital Payment Token Service. Available at: https://www.mas.gov.sg/regulation/notices/psn02-aml-cft-notice---digital-payment-token-service

- Monetary Authority of Singapore (MAS). (2023). MAS Stablecoin Regulatory Framework Announcement. MAS. Available at: https://www.mas.gov.sg/news/media-releases/2023/mas-finalises-stablecoin-regulatory-framework

- Pestalozzi Attorneys at Law. (2020). *Obtaining attachment on cryptocurrencies in Switzerland*. Available at: https://pestalozzilaw.com/en/insights/news/legal-insights/obtaining-attachment-cryptocurrencies-switzerland/legal_pdf/

- Reutlinger, M. (2021). Swiss Federal Court rules on selling of seized crypto assets. Reutlinger Rechtsanwälte. Available at: https://www.reutlaw.com/en/insights/swiss-federal-court-rules-on-selling-of-seized-crypto-assets

- S & P Global (2025). S&P Global Ratings: Stablecoin Regulation Gains Global Momentum, Available at: https://www.spglobal.com/ratings/en/research/articles/250210-stablecoin-regulation-gains-global-momentum-13400761

- Societe Generale. (2024). Societe Generale-Forge elevates its stablecoin to accelerate its distribution and free use [Press release]. Available at: https://wholesale.banking.societegenerale.com/

- Societe Generale-FORGE. (2023). CoinVertible (EURCV) Stablecoin – Product Page. Available at: https://www.sgforge.com/product/coinvertible/

- Societe Generale-FORGE. (2024). EUR CoinVertible (EURCV) Whitepaper as of October 1, 2024. Available at: https://www.sgforge.com/wp-content/uploads/2024/10/SG-Forge-EURCV-White-Paper-20241001.pdf

- Societe Generale-FORGE. (2025). Societe Generale-FORGE (SG-FORGE) advances its multichain strategy and selects the Stellar network to deploy its MiCA compliance stablecoin. Press release, Paris, February 20th, 2025. Available at: https://www.sgforge.com/stellar-network-stablecoin/

- Swiss Blockchain Federation. (2024). Statement on FINMA Guidance 06/2024. Available at: https://blockchainfederation.ch

- Swiss Code of Obligations. (2023). SR 220. Federal Act on the Amendment of the Swiss Civil Code. Available at: https://fedlex.data.admin.ch/eli/cc/27/317_321_377/en

- Swiss Criminal Procedure Code (StPO). (2023). SR 312.0. Available at: https://fedlex.data.admin.ch/eli/cc/2010/267/en

- Swiss National Bank (SNB). (2022). Annual Financial Stability Report. Available at: https://www.snb.ch/en/mmr/reference/stabrep_2022/source/stabrep_2022.en.pdf

- Sygnum Bank. (2020, March 31). Sygnum Bank launches digital CHF token (DCHF) [Press release]. Available at: https://www.sygnum.com/digital-asset-banking/digital-swiss-franc-dchf/

- Sygnum Bank. (2021, April 1). Introducing the Sygnum Security Token and tokenization smart contract suite. Available at: https://www.sygnum.com/blog/2021/04/01/introducing-the-sygnum-security-token-and-tokenization-smart-contract-suite/