International Telecommunication Union

DIGITAL CURRENCY GLOBAL INITIATIVE

TELECOMMUNICATION
STANDARDIZATION SECTOR

(11/2022)

Final report of the Stablecoins Workstream

Architecture, Interoperability Requirements and Use Cases (AIRU) Working Group

DISCLAIMER

The findings, interpretations, and conclusions expressed in this work do not necessarily reflect the views of Digital Currency Global Initiative partners, including the International Telecommunication Union, or Stanford University. The mention of specific companies, or of certain manufacturers' products does not imply that they are endorsed nor recommended by ITU in preference to others of a similar nature that are not mentioned. Errors and omissions excepted, the names of proprietary products are distinguished by initial capital letters. The Digital Currency Global Initiative partners do not guarantee the accuracy of the data included in this work. The boundaries, colours, denominations, and other information shown on any map in this work do not imply any judgment on the part of the Digital Currency Global Initiative partners concerning the legal status of any country, territory, city or area or of its authorities or the endorsement or acceptance of such boundaries.

About this report

This report was prepared by Dr. habil. Jean-Marc Seigneur, University of Geneva and Vice Team Leader of the Architecture, Interoperability and Use Cases Working Group of the Digital Currency Global Initiative, as part of the activities of the Stablecoins workstream. The author would like to acknowledge the contributions of the following persons below for their inputs to the report:

1. Mr. Thomas Boltshauser, University of Geneva
2. Mrs. Suzana Maranhão Moreno, University of Geneva
3. Adv. Gueorgui Gotzev, Lawyer, KOHLER GOTZEV
4. Dr. Guangbo Zhang, Web3 Capital

The author would also like to thank the members of the Digital Currency Global Initiative for their valuable inputs and comments received on the report and the ITU Secretariat.

Table of Contents

Table of Figures

1 Introduction

The purpose of this paper, which is part of the Digital Currency Global Initiative (DCGI), is to present to the Architecture Working Group a basis for discussion about stablecoins. To do this, Section 2 gives an overview of the definitions of stablecoins. Then, Section 3 presents a taxonomy to map the 9 existing projects that have been presented to the Architecture Working Group during 2020, 2021 and 2022 namely:

1. The GLX stablecoin use-case (Seigneur, 2020), which aims to provide a stablecoin protecting purchasing power based on a managed basket of fiat, chosen according to GDPR performance, and gold
2. The Ampleforth stablecoin use-case (Tan & Seigneur, 2020a), which is an algorithmic stablecoin aiming to remain stable with regard to 1 USD value according to the Consumer Price Index in 2019
3. The Dai stablecoin use-case (Tan & Seigneur, 2020b), which is pegged to 1 USD backed by cryptocurrencies collaterals on-chain via collateralized debt positions (CDP)
4. The BNDES stablecoin use-case (S. M. B. M. Moreno & Almeida, 2020), which aims to increase the public trust in the Brazilian Development Bank (BNDES) by tracking how the money of the bank is used
5. The Celo cUSD stablecoin use-case (Copic, 2020), which tracks the value of the U.S. Dollar
6. The Libra / Diem stablecoin use-case (Boltshauser & Seigneur, 2021a), which aimed to provide a coin stable with regard to a basket of fiat currencies and now 1 $ per Libra/Diem USD in partnership with a well-known authorized and regulated bank in the USA and the Libra/Diem association bootstrapped by Facebook
7. The USDT stablecoin use-case (Boltshauser & Seigneur, 2021b), which aims to maintain 1 $ per USDT based on a reserve of cash and other assets (treasury bills, commercial paper…) by a private company incorporated in Hong-Kong
8. The Lugh stablecoin use-cae (Lartigau, 2021), which aims to maintain 1 Euro per Lugh in partnership with a well-known authorized regulated French bank
9. The a-USD stablecoin on Acala Polkadot (Zhang, 2022)

We have compiled their key differences in a table in Section 4. Because it is an essential point for stablecoins, we have also discussed the legal frameworks of different influential jurisdictions in the world that are putting pressure on existing projects with regards to compliance in Section 5. Finally, Section 6 discusses interoperability and standardization areas.

2 What is a stablecoin?

To properly study stablecoins, we must first define what they are. This is a difficult exercise because their designs can vary greatly. For this purpose, we will first survey some definitions found in other reports or documents, highlighting their strengths and weakness. Then, we will provide our definition which will be used for the rest of the document.

First, there is a consensus on the existence of a price stabilization mechanism. This stabilization mechanism can then be classified in different ways. (Bolliger, 2019) suggests the following typology:

> *Based on their design, stablecoins have been classified into four types: (1) tokenized funds; (2) off-chain collateralized stablecoins; (3) on-chain collateralized stablecoins; and (4) algorithmic stablecoins" [5].*

In addition to the price stabilization and technical features, stablecoins can also be defined according to the scale on which they operate and so the risk they generate. For instance, the Financial Stability Board (FSB) (*FSB Consults on Regulatory, Supervisory and Oversight Recommendations for "Global Stablecoin" Arrangements*, 2020) describes stablecoins as:

> *a specific category of crypto assets that have the potential to enhance the efficiency of the provision of financial services, but may also generate risks to financial stability, particularly if they are adopted at a significant scale. Stablecoins are an attempt to address the high volatility of "traditional" crypto assets by tying the stablecoin's value to one or more other assets, such as sovereign currencies. They have the potential to bring efficiencies to payments and to promote financial inclusion. However, a widely adopted stablecoin with a potential reach and use across multiple jurisdictions (a so-called "global stablecoin" or GSC) could become systemically important in and across one or many jurisdictions, including as a means of making payments.*

The MIT Press (Lipton et al., 2020) has defined stablecoins through three aspects that include price stability but not only:

1. There must be some form of stabilization mechanism to reduce volatility relative to an existing currency.
2. Stablecoins have a market price of their own, implying that its price expressed in the target quote currency is not necessarily equal to one.
3. They argue that stablecoins should be technology-neutral excluding already existing distinct forms of currencies that simply use a Distributed Ledger Technology (DLT) for recording purposes. According to them, this would help to differentiate between stablecoins as a genuinely new form of money (e.g., DAI (Bhat et al., 2021)) and commercial bank money that is powered by new DLT (e.g., JPM Coin (*J.P. Morgan Creates Digital Coin for Payments*, 2019)).

However, we find their extended definition too restrictive. Although we agree that there must be some form of stabilization mechanism to reduce volatility, we consider that it can be relative to any reference point and not only to another currency (e.g., see the GLX basket coin use-case meant to be stable regarding purchasing power (Seigneur et al., 2017)).

(Bullmann et al., 2019), researchers of the European Central bank, have also a definition that encompasses a broader panel of types: "[...] stablecoins are digital units of value designed to minimize fluctuations in their price against a reference currency or basket of currencies".

Regardless of the type of mechanism used, the most important point is the stability of the coin. As we have seen, this stability is relative not to a particular asset or basket of assets but a specific reference point. That is why we suggest the following definition:

A stablecoin is a coin (i.e., one unit of an asset) whose value is stable relative to a reference, which may be some units of another asset or basket of assets or a more abstract reference like purchasing power.

3 Taxonomy of stablecoins

After defining what stablecoins are, it is necessary to draw up a typology that allows us to classify them and thus understand their diversity.

3.1 Models

The BIS (Bank for International Settlements) Working Papers No 905 (Arner et al., 2020) classifies stablecoins as following:

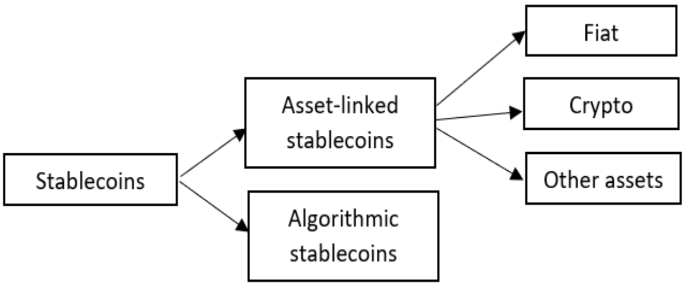

Figure 1. BIS classification of stablecoins

This typology is interesting because it essentially focuses on collaterals. However, the large variety of existing stablecoins requires a more complex system. To go deeper in detail, we will use the classification Framework for Stablecoin Designs (Moin et al., 2019). This typology has the advantage of covering a wide range of options while remaining fairly generalist.

However, this typology contains only elements directly related to the stabilization mechanism. To work properly, a stablecoin protocol also needs additional elements.

Below, in what we call the *main axes*, we will briefly describe each of these categories. Then, we will further enrich this typology with additional aspects, which we call the *secondary axes*.

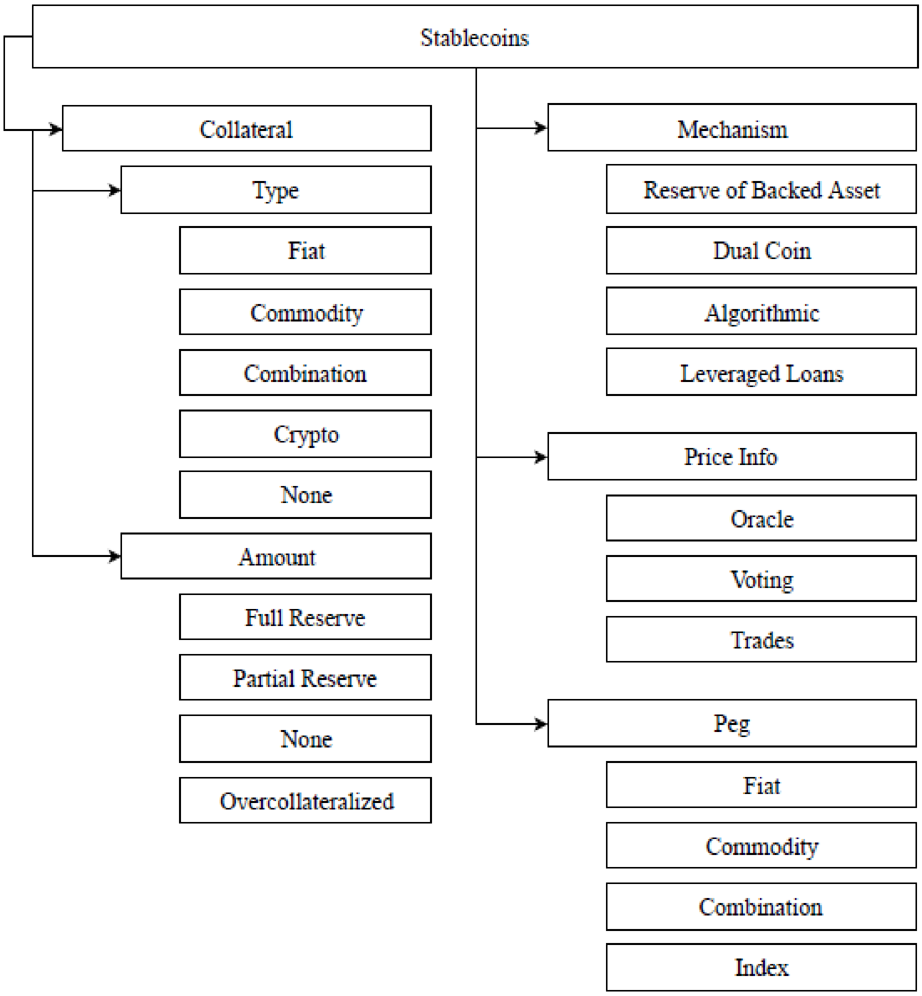

Figure 2. (Moin et al., 2019)' stablecoins taxonomy

The field of stablecoins is still expanding fast at time of writing and it clearly goes beyond to stablecoins referenced to fiat currencies as we can see in the recent diagram of new stablecoins projects by Nansen in Figure 3 (Loon, 2021).

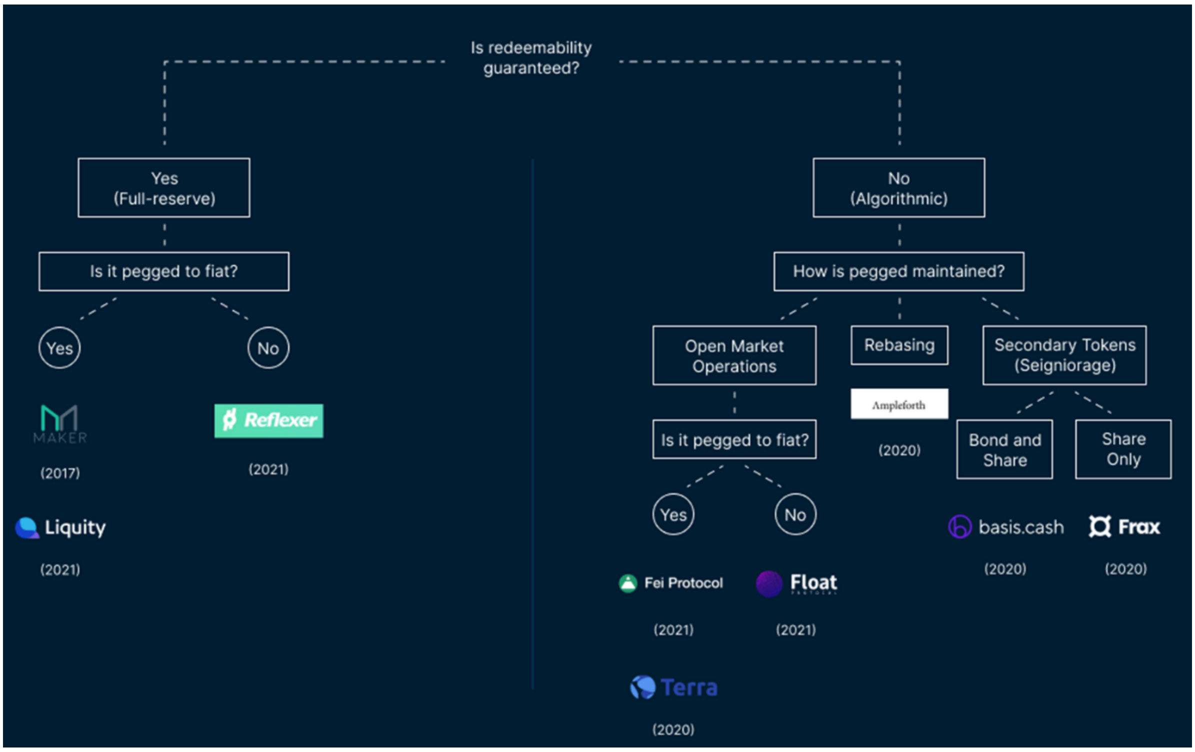

Figure 3. Algorithmic stablecoins overview

3.2 The main axes

The crucial point about stablecoins is how they stabilize their price. Some elements are directly related to this stabilization strategy. We have grouped them under the term “main axes”.

3.2.1 Collaterals

Collaterals are the assets kept in a reserve to guarantees that the stablecoin can be redeemed at a fixed minimum price. This reserve raises questions about security and transparency.

These collaterals can be:

- **Fiat:** Cash or cash equivalent can be kept in the reserve. This reserve is often a commercial bank, but it can also be a private vault. These assets are off-chain. There are different types of cash equivalent that are more or less risky. For example, treasury bills are usually considered less risky than
- **Commodity:** Depending on commodities, they can also be kept in banks or private vaults. These assets are off-chain.
- **Combination:** The reserve can keep a mix of commodities and national currencies.
- **Cryptocurrencies:** These assets can also be digital rather than physical. In this case, there is no need for a safe deposit box or a bank. Locking crypto-currencies in a smart contract (which acts as a digital safe) is a convenient solution. However, cryptos themselves are very volatile. These assets are on-chain.
- **None:** A stablecoin may not be collateralized. This is the case with algorithmic stablecoins. Other mechanisms must be used to ensure that the price of a token cannot fall below a certain limit.

The amount of these collaterals can be:

- **Full reserve:** This means that for every coin in circulation there is the exact equivalent in fiat currency kept in the reserve.
- **Partial reserve:** If the mass of tokens in circulation is large, it is possible not to fully back a stablecoin. For instance, Tether initially said it was 100% fully backed by US dollars in their reserve but then they recently published but it is far less than that. Also, fully collateralized stablecoins which keep their assets in a commercial bank are partially collateralized due to the fractional reserve system of banks. The key point is to always have enough on hand to meet the demand.
- **Overcollateralized:** Some projects, especially those that lock cryptos into smart contracts, hold more assets than they issue tokens to cope with possible large price swings.

3.2.2 Stabilization mechanism

If the stablecoin has a reference point for its value, eventually with some assets in reserve as guarantees, it needs a mechanism that constantly adjusts the price to stabilize it.

- **Reserve of backed asset**: If the stablecoin can be redeemed for a fixed price thanks to assets held in a reserve and if it can be bought for a fixed price, so the value of the stablecoin will be relatively stable. In some cases, arbitrageurs earn money while helping maintain the peg.
- **Dual coins:** Another way to maintain stability is to issue two coins A & B. When token A's price is smaller than the value on which it is pegged, users and arbitragers can send token A to the system and receive A's worth of B. This reduces the supply of A and therefore increases its value. In the same way, when token A's price is bigger than the value on which it is pegged, users and arbitragers can send A's worth of B to the system and receive A.
- **Algorithmic:** Algorithmic stablecoins use mathematical mechanisms to adjust the supply of the tokens in circulation to stabilize their values. The recent $40 billion collapse of the Terra token and associated UST stablecoin (Shin, 2022; Yaffe-Bellany & Griffith, 2022) has shown that much more work is needed not only at the technical level to validate the resistance in case of crash but also at the social level. Terra UST was mainly controlled by the founder who managed to market himself as trustworthy. Even if he had been trustworthy, he was a central point of failure, which is odd for a solution aiming at being decentralized. aUSD has also experienced a major attack and fell very low from its 1$ peg even if so far it seems to have recovered (Dalton, 2022).
- **Leveraged loans:** In this approach, stablecoins are issued when users lock assets (often crypto-assets), in collateralized debt positions (CDPs). If the value of cryptocurrencies locked in the smart contract drops too much, users must block more cryptos to support the stablecoin price. Otherwise, the funds may be automatically liquidated by the platform or be decreased due to a penalty.

3.2.3 Price information

Stabilizing the value of a stablecoin requires being able to track the price evolutions of the asset(s) on which we are pegged.

- **Oracle:** It is an external source that provides a data stream that stablecoins issuers trust. To avoid attacks, several sources should be checked and compared.

- **Voting:** A vote is sometimes used to determine the value of the asset on which the stablecoin is anchored. There are incentives to give the most accurate value possible. It is also called crowd oracle or Schelling point mechanisms.
- **Trades:** Without external sources, prices are sometimes measured using only user's trades.

- **Settlement:** defined the issuer and settlement parties.

3.2.4 Peg (Reference points)

- **Fiat**
  Mostly, Stablecoins are pegged to a national fiat currency. Preferred currencies are those with the best reputation for stability as USD, EUR, JPY, or CHF.
- **Commodities**
  Sometimes, a commodity is used as a reference point. Gold is often favored.
- **Combination of currencies and/or commodities**
  Multiple currencies and/or commodities can also be mixed to give a reference point less dependent on a single item.
- **Index**
  A stock market index shows the course of an index that aggregates several stock markets values. Stablecoins can use an index as a reference point.

3.3 The secondary axes

To frame this stabilization strategy, other elements are required. We have grouped them under the term "secondary axes". They are not directly related to the stabilization of the token but are nevertheless essential to understand its functioning.

- **Underlying DLT:** The decentralized ledger technology infrastructure on which the stablecoin protocol is built.

- **Consensus mechanism:** The rules and procedures by which a consensus about the state of the ledger is reached among nodes.

- **Governance:** The rules and procedures by which the protocol is managed and changed.

- **Issuer:** The entity issuing the stablecoin.

- **Custodial:** The trusted third party that holds the assets.

- **Insurance:** The technical and legal mechanisms that protect stablecoin users and investors.

- **Interoperability with other digital currencies (DC):** The mechanisms to exchange the stablecoin with other crypto-currencies without the need for a centralized exchange.

- **Integration with other payment systems:** The bridges allowing interactions between the stablecoin and other cryptocurrencies on different blockchains and/or fiat currencies on traditional payment systems.

- **Storing and exchanging coins:** The potential devices allowing to conserve the stablecoins.

- **Freezing:** Some stablecoins have a method in their smart contract that allows the administrators or governance token holders to freeze the coins on specific addresses.

- **KYC/AML:** Some stablecoins may require that the addresses have passed Know Your Customer (KYC) and Anti-Money Laundering (AML) checks. The section below on the legal aspects underlines that they may be forced to integrate KYC/AML in many jurisdictions in the near future to be compliant.

- **Level of decentralization:** Given the above axes, it is clear that stablecoins are more or less decentralized, for example, if they ony allow addresses that have passed KYC/AML or are supposed to have assets in offline reserves or able to freez coins…

- **Systemic importance:** The potential systemic worldwide impact of the stablecoin.

3.4 Analysis of the presented use-cases

In this section, we break down 8 of the 9 study cases presented during the ITU meetings using the categories described above. This will allow us to have a practical and empirical point of view and to highlight the diversity of existing projects.

	Ampleforth [AMPL]	**Celo [cUSD]**	**Dai**	**Globcoin [GLX]**
Peg / Reference point	Fiat [1 AMPL = 1 USD according to the Consumer Price Index in 2019]	Fiat [1 cUSD = 1 USD]	Fiat [1 DAI = 1 USD]	Global reserve currency index (to simplify purchasing power)
Collaterals	None	Crypto-currencies / overcollateralized (initially of Celo's native asset (CELO), as well as other liquid cryptocurrencies like Bitcoin and Ether)	Crypto-currencies / overcollateralized	Basket of fiat currencies plus gold / full reserve
Stabilization mechanism	Algorithmic	Algorithmic	Leveraged loans	Reserve of backed asset
Price information	Oracles	Oracles	Oracles	Oracles
Underlying DLT	Ethereum	Celo blockchain	Ethereum	Ethereum
Consensus mechanism	PoW/PoS of Ethereum	PoS with BFT	PoW/PoS of Ethereum	PoW/PoS of Ethereum
Governance	On-chain governance mechanism based on community voting with the FORTH tokens	On-chain governance mechanism: proposals voted on by CELO holders using a weighted vote based on the same locked CELO commitment used to vote to elect validators	On-chain governance mechanism based on community voting with MKR tokens	Centrally managed by the private company

	Ampleforth [AMPL]	Celo [cUSD]	Dai	Globcoin [GLX]
Issuer	Ampleforth protocol	Celo protocol	MakerDAO	Reserve Currency Solutions – Swiss private company
Custodial	Non-custodial	Custodial but its public addresses are available on https://celoreserve.org/ so that anyone can audit the reserve	Non-custodial (the crypto collaterals are automatically managed by smart contracts)	Custodial
Insurance	None	None	Decentralized insurance pool (with limited power, in case of a major crash it may not be sufficient)	None
Interoperability with other DC	Can be swapped with other ERC-20	Can be swapped with other ERC-20	Can be swapped with other ERC-20	Can be swapped with other ERC-20
Integration with other Payment systems	To some extent compatible with other blockchains with bridges to Ethereum	Bridges with Bitcoin, Cosmos and Ethereum	To some extent compatible with other blockchains with bridges to Ethereum	To some extent compatible with other blockchains with bridges to Ethereum
Storing and exchanging coins	ERC-20 numerous compatible wallets and exchanges (amount of coins may be change due to rebase in case the value is far from the reference point)	Self-custodied wallet (Valora) and other third pary compatible wallets	ERC-20 numerous compatible wallets and exchanges	ERC-20 numerous compatible wallets and exchanges
Freezing	AMPL smart contract doesn't seem to have freezing so far but as it is been deployed as a proxy whoever deployed the smart contract could in theory arbitrarily add functions that allow for account freezing	cUSD could be frozen on an address but only in case of a successful governance vote by Celo community	No (the Dai smart contract doesn't have the freezing functions)	The private company has the fiat currencies and gold under its control in its reserve
KYC/AML	None in the current version of the smart contract that may be updated via proxy	No KYC/AML below 1000$ on the Celo Valora wallet	None (the current Dai smart contract cannot be updated to enforce KYC/AML)	None in the current version but the private company could easily enforce KYC/AML when wanted as it

	Ampleforth [AMPL]	Celo [cUSD]	Dai	Globcoin [GLX]
				controls the reserve
Level of decentralization	Medium (although the current version of the smart contract doesn't a freeze option, it may change due to proxy; the oracle requires the monthly offchain price from the centralized USA Bureau of Economic Analysis; no KYC/AML needed so far)	Low (smaller scale blockchain than Ethereum; combination of PoS and BFT with an alliance but initially pushed by cLabs)	High (the smart contract cannot be updated and don't have freezing or KYC/AML, the governance is quite decentralized thanks to the MKR governance tokens)	Low (the reserve of pegged assets is offchain controlled by a unique private company with promises of external periodic audits)
Systemic importance	Although this version may not be perfect, algorithmic stablecoins may create quite a systemic impact because they aren't pegged to fiat reserves	Although it has already an interesting reach on financial inclusion and with its mobile approach, its adoption is much lower than USDT or USDC that are the leaders in this category so far	Although this version may not be perfect, Dai has already played a systemic role for the adoption of decentralized finance (DeFi) and has still good potential due to its high decentralization level	Although the private company behind the GLX is small, having a periodically rebalanced basked of fiat currencies based on their GDP with purchasing power as reference point could create a systemic impact if allowed and adopted on a large scale

Figure 4 Stablecoins uses cases axes comparison table (Part 1)

	Libra/Diem	Tether [USDT]	BNDES	LUGH [EURL]
Peg / Reference point	Fiat [ex: 1 ≋USD = 1 USD]	Fiat [1 USDT = 1 USD]	Fiat [1 BNDES = 1 BRL]	Fiat [1 EUR-L = 1 EUR]
Collaterals	Fiat / full reserve	Fiat / partial reserve	Fiat / full reserve	Fiat / full reserve
Stabilization mechanism	Reserve of backed asset	Reserve of backed asset	Reserve of backed asset	Reserve of backed asset
Price information	Oracles	Oracles	Defined by BNDES, which is the issuer / settlement body with no secondary market	Oracles
Underlying DLT	Libra Blockchain	Mainly Ethereum & Tron but available on several blockchains	Ethereum	Tezos

Consensus mechanism	Libra BFT	PoW/PoS of Ethereum or PoS of Tron	PoW/PoS of Ethereum	PoS of Tezos
Governance	Managed by the Libra / Diem consortium	Centrally managed by the private company	Centralized at BNDES	Relies onto 4 administrators groups (Owner, Administrator, Minter, Reserve) using multi-signatures to operate EUR-L
Issuer	Libra / Diem Association in partnership with Silvergate bank	Tether Ltd – private company	BNDES bank	Private company
Custodial	Custodial	Custodial	Non-Custodial	Custodial
Insurance	High regulatory compliance enforcing government-issued ID for the Novi wallet that states that "in event of fraud, you will be eligible to receive a full refund"	None	BNDES is a state-owned institution.	None
Interoperability with other DC	Claim to develop new standards that developers will be able to use	Can be swapped with other ERC-20	No (it may be possible in the future, for settlement)	Can be swapped with other Tezos-based FA1.2 tokens
Integration with other Payment systems	Not released yet	Massively compatible: Ethereum / OMG network / Binance Smart Chain / Tron / Solana	Some integration with SPB (Brazilian Payment System)	Partnership with the bank Société Générale
Storing and exchanging coins	Libra/Diem-compatible wallets, especially the Facebook Novi wallet, a reference wallet implementation is provided for other providers	ERC-20 compatible wallets and many major centralized exchanges	ERC-20 compatible wallets	FA1.2 compatible wallets
Freezing	The Libra/Diem can freeze addresses	Yes Tether can freeze addresses	Yes, at least in the beginning.	The administrators group has the ability to declare an address as accredited, to lock/unlock an address, to pause transfer and to transfer from one address to another

KYC/AML	Any account on the Facebook Novi wallet will required government IDs	No KYC/AML so far	De facto compliance reusing trust from national digital certificate	Yes for now as it is restricted to trade on centralized exchanges where users have to pass KYC
Level of decentralization	Low (run on its own controlled blockchain with freezing feature; although the consortium members are quite diverse and influent, they have mainly been centrally chosen by Facebook to some extent; only addresses that have passed KYC/AML with government ID on Novi wallet)	Low (although it runs on several blockchains without KYC/AML, Tether can freeze any addresses and is the unique controlling party with opaque information regarding its reserve, which is rarely audited and not in-depth, transparently)	Low (deployed on Ethereum but with centralized governance by BNDES)	Low (although it runs on the quite decentralized Tezos blockchain, it relies on 4 administrators group that have the ability to freeze addresses)
Systemic importance	Although the decentralization is low, the level of the technical team is high and Facebook and consortium members already have more than 1,5 billion users	It is the most used stablecoins with links to several exchanges with high leverage, which is clearly a high systemic risk for crypto-currencies, at least on the short term after a potential cease and desist of Tether by the USA	Until now it has only been used on pilot projects	Until now it is only a pilot project but it is interesting as it is launched in France, which has specific stablecoins views, by one of the major supermarkets groups.

Figure 5 Stablecoins uses cases axes comparison table (Part 2)

3.5 Applicability to NFT

NFTs (Non-Fungible Tokens) are special digital tokens that are not fungible. The most well-known de facto standard is the ERC-721 (Entriken et al., 2018) that is used to generate NFT on the Ethereum blockchain. In 2021, the NFT market got a lot of momentum thanks NFT used to trade digital art being images, animations, video clips or music.

In the ERC-721 standard, the assets themselves, for example, an image, are not embedded into the NFT but linked thanks to a URL, which may lead to a file on cloud-based Web server or on a peer-to-peer file system such as IPFS (*IPFS Powers the Distributed Web*, n.d.).

A NFT can also be linked to a digital asset corresponding to a piece of a real-estate or a specific financial asset.

At least in theory, our stablecoin definition can be applied in the case of an NFT linked to a financial asset because the coin is stable with regard to the linked asset. In practice as mentioned above, the link may become broken, for example, due to the Web server hosting the digital asset that goes down. A file on IPFS may disappear too if no peer wants to maintain the file for sure. **However as the hash of the digital asset should remain the same, the digital asset could be uploaded again and then retrievable again on IPFS. So, at the difference of a fungible token that keeps the value of the token it belongs to, an NFT may lose its reference value.** In the standardisation below, we draft some recommendations regarding which fields and information an NFT should have to lower the risk of such issue. For example, the hash of the digital asset could be added as text in the NFT to be able to verify the digital asset it is linked to.

There is another issue regarding the current state of NFTs. Although the ownership of a fungible token ensures its authenticity, anybody can create a NFT. Without knowing the real identities behind the addresses who have created or are involved with the NFT, the authenticity of the NFT is unsure. For example, in the case of NFT linked to digital art, someone may create an Ethereum address to mint some NFTs and claim it is the real artist. Even if the real artist has created the Ethereum address, if she/he dies afterwards without leaving proofs that she/he created the address. There will be no proof that the generated NFT are authentic digital arts created by the dead artist. A mechanism to prove the real identity of the NFT creator or that the initial asset owner has agreed to transfer the ownership of the asset is therefore necessary. If we continue our example in the digital art domain, even if there is a proof that the address used to create the NFT is owned by the artist, there is a need to know further legal information such as the rights given to the buyer and the rights kept by the artist, ideally mentioning how many other versions of the art may be created in the future.

A final problem arises when the asset linked to a NFT isn't digital and doesn't have an easy to check hash. Physical assets may then be verified thanks to a RFID chip embedded in the asset or the recognition of its shape. Unfortunately, all of these verifications techniques aren't perfect and cheating risks remain for physical assets linked to NFTs.

4 Compliance

We discuss below the legal aspects of stablecoins in several important jurisdictions in the field.

4.1 United States of America

In the USA, a bill about stablecoins is currently being discussed: the so-called Stablecoin Tethering and Bank Licensing Enforcement act (STABLE act) (*Tlaib, García and Lynch Introduce Legislation Protecting Consumers from Cryptocurrency-Related Financial Threats*, 2020). It was proposed by the American Congress, more precisely by three representatives led by Rashida Tlaib on December 2, 2020.

Companies that issue stablecoins must comply with Anti-Money Laundering (AML) and Know Your Customer (KYC) regulations and must register as:

- Money Service Business (Fincen) – on the Federal level
- Money Transmitter – on the State level

This bill requires stablecoin-issuing companies to:

1. obtain a banking license.
2. comply with existing banking regulations.
3. obtain approval from the Central bank, the FDIC, and the appropriate banking agency 6 months before its issuance and maintain an ongoing analysis of potential systemic impacts and risks.
4. maintain sufficient reserves of dollars on deposit with the Central bank. All tokens issued would have to be convertible into dollars at any time. Or otherwise, to obtain FDIC insurance.

According to Rashida Tlaib, the purpose of this bill is to "Preventing cryptocurrency providers from repeating the crimes against low- and moderate-income residents of color traditional big banks have is critically important" (*Congresswoman Rashida Tlaib sur Twitter*, 2020). The STABLE act has not yet passed.

In the bill, the definition of the stablecoins is the following one:

> The term stablecoin means any cryptocurrency or other privately-issued digital financial instrument that – (A) is directly or indirectly distributed to investors, financial institutions, or the general public; (B) is (i) denominated in US dollars or pegged to the US dollars or (ii) denominated in or pegged to another national state currency and (C) is issued (i) with a fixed nominal redemption value; (ii) with the intent of establishing a reasonable expectation or belief among the general public that the instrument will retain a nominal redemption value that is so stable as to render the nominal redemption value effectively fixed or (iii) in such a manner that, regardless of intent, has the effect of creating a reasonable expectation or belief among the general public that the instrument will retain a nominal redemption value that is so stable as to render the nominal redemption value effectively fixed.

According to her bill, a stablecoin is a cryptocurrency pegged to fiat(s) and that creates an expectation about a fixed redemption value. We have seen in our discussion of definitions in Section 2 that it is a limited view of the different types of stablecoins.

Finally, *stablecoin-related commercial activities* are also concerned by the bill. However, it is not clear whether operating a node for free (as many full nodes do) counts as "stablecoin-related commercial activity" if done on a non-commercial basis. A more recent bill called the US infrastructure bill (*Sam Bankman-Fried Breaks down How the Crypto Tax Provision in the Infrastructure Bill Could Force Swaths of the Industry out of the US | Currency News | Financial and Business News | Markets Insider*, 2021) has added a section on crypto-currencies and decentralized finance (DeFi) focusing on KYC requirements for crypto transactions that may require intermediaries like miners, validators or DeFi providers who usually do not bother about KYC to be considered as brokers and have to enforce KYC. It may be impossible for them due to technical/costs reasons but anyway mandatory if they do not want to become illegal. The goal is also to be able to tax crypto transactions. (S. M. B. M. Moreno et al., 2021) give an overview of crypto transactions KYC and AML.

4.2 European Union

On 24 September 2020, the European Commission submitted a new regulatory framework regarding financial technologies (Digital Finance package) aiming to provide a licensing regime in Europe by 2024. Such a unified approach instead of a fragmented one, aims to simplify the rules and improve the competitiveness of European fintech companies while protecting consumers and financial stability.

A crucial part of this new package is a draft legal and regulatory proposal, an EU Regulation to recognize and govern crypto-assets called Markets in Crypto-Assets (MiCA) (*Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 COM/2020/593 final*).

We remind first what means legal tender. The Euro is the official currency of 19 European Union countries which collectively make up the Euro area, also known as the Eurozone. Within the Euro area, the Euro is the only legal tender. In the absence of a specific agreement concerning the means of payment, creditors are obliged to accept payment in Euros. Parties may also agree to transactions using other official foreign currencies (e.g. the US dollar). They may also agree to use privately issued 'money' like local exchange trading systems (e.g. voucher-based payment systems) or virtual currencies (e.g. Bitcoin).

Article 128 (1) Treaty on the Functioning of the European Union lays down the legal tender status of Euro banknotes, and article 11 of Regulation EC/974/98 (Article 128 (ex Article 106 TEC) 1. The European Central Bank shall have the exclusive right to authorise the issue of Euro banknotes within the Union. The European Central Bank and the national central banks may issue such notes. The banknotes issued by the European Central Bank and the national central banks shall be the only such notes to have the status of legal tender within the Union. Below are the recommendations of the Commission in 22 March 2010 on the scope and effects of legal tender of Euro banknotes and coins. Common definition of legal tender consists of where a payment obligation exists, the legal tender of euro banknotes and coins should imply:

(a) Mandatory acceptance:

The creditor of a payment obligation cannot refuse euro banknotes and coins unless the parties have agreed on other means of payment.

(b) Acceptance at full face value:

The monetary value of euro banknotes and coins is equal to the amount indicated on the banknotes and coins.

(c) Power to discharge from payment obligations:

A debtor can discharge himself from a payment obligation by tendering euro banknotes and coins to the creditor.

As part of this package the EU Commission has provided for a legal framework for an equally important EU Regulation for a pilot regime for Distributed Ledger Technology (DLT) (*Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Pilot Regime for Market Infrastructures Based on Distributed Ledger Technology*, 2020) and a revision of the Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds to extend its requirements, commonly designated as the "Travel rule" to MiCAR in the light of near future enactment.

In this context, a Regulation is a legislative act of the European Union that is immediately enforceable and binding in its entirety and directly in each EU member state without the need of national implementing measures. A EU Regulation prevails and over any conflicting domestic provisions and can be invoked in front of domestic courts.

On 14th of March 2022, the European Parliament adopted its negotiating position on MiCA. Currently the draft MiCAR is in the legislative process of first reading with the European Parliament.

The draft MiCAR is based on the legal and regulatory architecture already commonly known to all financial market participants as MIFID2 and MIFIR in the sense that it regulates the Crypto-Assets (products), the services on such assets and the entities that car provides such services to the public.

Furthermore, the EU approach is that substance prevails over form. Therefore, crypto assets that have the characteristics of a financial instrument or e-money are governed by the respective EU legal framework under MIFID2 and Prospectus regulation on one side and the electronic money institutions directive on the other side.

Amongst others, Article 3,1. provides for the definitions of crypto assets and their taxonomy, six of which are covered for the purpose herein:

- **"Crypto-assets"** are a digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology (Article 3,1. (2));
- **"Asset-referenced tokens"** are a type of digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology that purports to maintain a stable value by referring to the value of several fiat currencies that are legal tender, one or several commodities or one or several crypto-assets, or a combination of such assets (Article 3,1. (3));
- **"Electronic money tokens" or "e-money token**" a type of digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology the main purpose of which is to be used as a means of exchange and that purports to maintain a stable value by referring to the value of a fiat currency that is legal tender (Article 3,1. (4));
- **"Utility tokens"** are a type of crypto-asset which is intended to provide digital access to a good or service, available on DLT, and is only accepted by the issuer of that token (Article 3,1. (5));
- **"Issuers of crypto-assets"** are a legal persons who offer to the public any type of crypto-assets or seek the admission of such crypto-assets to a trading platform for crypto-assets (Article 3,1. (6)); and
- **"Crypto-asset service provider"** is any person whose occupation or business is the provision of one or more crypto-asset services to third parties on a professional basis (Article 3,1. (8)).

In general, crypto-asset service providers shall have to receive prior authorization (the MiCA CASP license) from competent member state governments, which will be valid across the European Union.

Asset-referenced tokens and Electronic money tokens are governed by respectively Title III and Tittle IV of MiCAR. MiCA document does not use the term “stablecoin” but stablecoins are thus qualified as asset-referenced tokens or e-money tokens.

Asset-referenced tokens aim at stabilizing their value by reference to several fiat currencies, to one or more commodities, to one or more other crypto-assets, or to a basket of such assets. They could therefore be widely adopted by users to transfer value or as a means of payments and thus pose increased risks in terms of consumer protection and market integrity compared to other crypto-assets. Issuers of asset-referenced tokens should therefore be subject to more stringent requirements than issuers of other crypto-assets.

So-called algorithmic "stablecoins" that aim at maintaining a stable value, via protocols, that provide for the increase or decrease of the supply of such crypto-assets in response to changes in demand should not be considered as asset-referenced tokens, provided that they do not aim at stabilizing their value by referencing one or several other assets.

The issuers of asset-referenced tokens must, *inter alia*:

- Have their registered office in the European Union;
- Be authorized by the competent national authority; and
- Produce a crypto-asset white paper on asset-referenced tokens should include clear, fair and not misleading information on the stabilization mechanism, on the investment policy of the reserve assets, on the custody arrangements for the reserve assets, and on the rights provided to holders.

The issuers of e-money tokens must, *inter alia*:

- Have their registered office in the European Union;
- Be authorized either as a credit institution under Directive 2013/36/EU or as an electronic money institution under Directive 2009/110/EC and they should comply with the relevant operational requirements of Directive 2009/110/EC;
- Produce and notify to their competent authority, a crypto-asset white paper that contains all the relevant information concerning that issuer and the offer of e-money tokens or their admission to trading on a trading platform for crypto-assets that is necessary to enable potential buyers to make an informed purchase decision and understand the risks relating to the offer of e-money tokens. The crypto-asset white paper should also explicitly indicate that holders of e-money tokens are provided with a claim in the form of a right to redeem their e-money tokens against fiat currency at par value and at any moment.

If utility tokens are issued for a value superior to 1 million EUR, the issuers have to publish a whitepaper and transmit it to the legal authorities (which don't need to accept it).

The regulation is stricter for stablecoins. Indeed, in addition to publishing a whitepaper, asset-referenced token companies' issuers must be authorized and overwatched by a regulation authority if their initial coin offering (ICO) is more than EUR 5 million. Also, the asset reserve that stabilizes the value will have to follow some requirements.

Further requirements could be required (e.g., the amount of capital) depending on the appreciation of the European Banking Authority (EBA).

Most recently, focus has been made on the draft amendment of the aforementioned Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds as the contemplated amendment aims at extending the so called "Travel Rule" requirements of the FATF Recommendations on Virtual Assets and Virtual Assets Services Providers to the issuers or services providers of crypto-assets in the European Union. The requirements consist of collecting mandatory personal information from the seller and buyer of crypto-assets by the crypto service providers and/or issuers. The stakes are high as in it is currently under discussion to enforce different monetary thresholds for crypto-assets that are much stricter than the one applicable to tradition money transfers in the SEPA zone.

4.3 China

The People's Bank of China has started to work on its Central Bank Digital Currency (CDBC) much before all other countries. They have invested money to be able to carry out serious research and development. For example, they defined the requirement for dual offline payment of its CBDC as early as March 2016 when they a patent called "method and system for offline payment adopting digital currency chip card" (*Three Schemes for Dual Offline Payment of CBDC, Says China's Central Bank | NEWS.8BTC.COM*, 2020). A solution for offline use of existing stablecoins implemented as ERC-20 is presented in (Seigneur, 2019).

According to a revised draft of the "People's Bank of China Law", published on 23 October 2020, Digital Currency (DC) / Electronic Payment (EP) is now considered as legal tender in China. Article 22 stipulates that "no unit or individual may produce or sell tokens, coupons and digital tokens to replace RMB in circulation in the market" (Bharathan, 2021). Thus, any stablecoin pegged to the RMB is likely to have major issues with China because they don't have the official authorization.

In 2021, different Chinese entities disapproved of existing non-stablecoin cryptocurrencies such as Bitcoin. The National Internet Finance Association of China, the China Banking Association and the Payment and Clearing Association of China, publish a joint statement to remind that they must not provide any services related to cryptocurrencies. On 21 May 2021, a statement from the Chinese Vice Premier Liu He, claims that it is necessary to "crackdown on Bitcoin mining and trading behaviour, and resolutely prevent the transmission of individual risks to the social field" (Cox, 2021). Following this, the Inner Mongolia region drafted eight measures to ban crypto mining (Zhao, 2021). Other Chinese regions where mining is intensive due to cheap electricity price has followed the same path. One hand, given the large Bitcoin mining share of Chinese miners, the Bitcoin price drop at that time is likely to have been correlated. On the other hand, it may have contributed to decentralize the location of Bitcoin miners in the world.

4.4 Switzerland

In Switzerland, authorities have considered that the current legal framework provides already adequate regulation on crypto-currencies. However, some adaptations have been made via the DLT Act (*Federal Council Brings DLT Act Fully into Force and Issues Ordinance*, 2021).

The type of regulation that applies to crypto-assets depends on their designation. According to FINMA (*La FINMA publie un guide pratique sur les ICO*, 2018), the Swiss financial regulator, tokens can belong to 3 different categories (or be a hybrid of several):

1) **Payment tokens:** Also called cryptocurrencies, they are tokens that are intended to be used, now or in the future, as a means of payment for acquiring goods or services or as a means of money or value transfer. Cryptocurrencies give rise to no claims on their issuer.
2) **Utility tokens:** Tokens that are intended to provide access digitally to an application or service using a blockchain-based infrastructure.
3) **Asset tokens:** Assets such as debt or equity claim on the issuer. Asset tokens promise, for example, a share in future company earnings or future capital flows. In terms of their economic function, therefore, these tokens are analogous to equities, bonds or derivatives. Tokens that enable physical assets to be traded on the blockchain also fall into this category.

Besides relevant AML regulation, securities regulations must apply if tokens are considered as securities under Swiss law. It is determined on a case-by-case basis by FINMA and tokens marketed as utility tokens may be requalified as security tokens, for example, if at time of selling the system wasn't finished and the investors expected that the developers would finish the system thanks to the money raised. For example, according to (Haeberli et al., 2021), the following regulations may apply:

- Swiss securities firm license requirements under the Financial Institutions Act (FinIA)
- Swiss trading platform regulations under the Financial Markets Infrastructure Act (FMIA)
- Swiss prospectus requirements and further regulations in connection with financial services under FinSA

According to FINMA, stablecoins aren't considered as a fourth category just because they have the goal to minimize price volatility. Furthermore, given that the concrete design of stablecoins can vary greatly in legal, technical, functional, and economic terms, no generic classification is possible. FINMA provides the following table to better understand how they analyze stablecoins projects (*FINMA Publishes 'Stable Coin' Guidelines*, 2019).

Categories	**Indicative supervisory classification (in addition to anti-money laundering legislation)**
1) Linked to fiat currency / cryptocurrency with fixed redemption claim	Deposit under banking law
2) Linked to basket of fiat currencies / cryptocurrencies with redemption claim dependent on price development	Management of the currency basket and risk-bearing: – for the account of the issuer: deposit under banking law – for the account of the token holder: collective investment scheme
3) Linked to commodity (incl. "bank precious metals") with contractual claim	Bank precious metals: deposit under banking law Commodity: security and possibly derivative
4) Linked to basket of commodities (incl. "bank precious metals") with redemption claim dependent on price development	Collective investment scheme
5) Linked to commodities (incl. "bank precious metals") with ownership rights	No prudential licensing requirement
6) Linked to real estate with redemption claim dependent on price development	Collective investment scheme
7) Linked to specific security with contractual claim	Security and possibly derivative
8) Linked to basket of securities with redemption claim dependent on price development	Collective investment scheme

Figure 6 FINMA stablecoins relevant regulations table

4.5 KYC and AML Compliance Verification on User Transactions

The Financial Action Task Force (FATF) (*FATF-GAFI - Financial Action Task Force*, n.d.) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF has developed a series of recommendations that are recognized as the international standard for combating money laundering and other related financial crimes. FATF recommendations include preventive measures that apply to traditional financial systems and virtual asset service providers. Countries that follow FATF recommendations must promote measures to make these recommendations a reality in the public and private sectors. Two sets of regulations are relevant in the context of compliance verification on user transactions involving cryptoassets: usual KYC/AML regulation and, more recent, the travel rule. Both are verified by intermediaries.

According with travel rule, the ordering/beneficiary VASP (virtual asset service provider) involved in a cryptocurrency transfer shall obtain and hold required and accurate originator and beneficiary information. It is not necessary for the information to be attached directly to the cryptocurrency transfer itself. Several industry consortiums are currently working on a technological solution to solve the challenges induced by the compliance with the Travel Rule. Amongst the leading ones are: OpenVASP (*Open Vasp – An Open Protocol to Implement FATF's Travel Rule for Virtual Assets*, n.d.)and the Travel Rule Information Sharing Architecture called (*Trisa.Io Travel Rule Compliance – FATF Guidance*, n.d.).

VASPs are intermediaries involved in virtual assets transfers. Regulations based on intermediaries cover only part of cryptoasset transactions because DLT/blockchain enables the possibility of performing transactions without involving intermediaries if done between two self-hosted wallets. There is no recommendation, regulation or technical solution in place focusing on these transactions, as far as the authors know. There is an ongoing discussion if and how the self-hosted wallet transactions should be monitored by regulators. Until now, FATF is not explicitly giving a broad recommendation to regulate transactions among self-hosted wallets because (a) the available data on the P2P market is not reliable enough to make an informed policy decision, (b) The intermediated transactions are still relevant enough to allow for effective implementation of the standards and (c) P2P transactions that are visible on public ledgers enable financial analysis and law enforcement investigations (Notabene, 2022).

A technical proposal for voluntarily regulation that cover all types of wallets, including self-hosted ones, is depicted in Figure 6 and can work in a complementary way to existing intermediary-based regulations. This approach enables self-hosted wallet users to participate in regulated use cases, including institutional DeFi like Aave Arc. In addition, this approach empowers users to take more informed decisions considering the intrinsic risks of their own transactions. Some guidelines considered in the design of this model are: (a) Work on all types of wallets, on-the-fly, without relying on intermediaries or a single verifier; (b) is backward-compatible with existing on-chain code and with existing DLT/blockchain networks; (c) preserve evidence that verification was done, verifiable for any external observer, and do not include PII (personal identifiable information) on-chain; (d) minimize the disclosure of PII while respecting specific national regulations; (e) enable the development of new use cases compliant-by-design with KYC/AML requirements with on-chain verification; (f) do not block any transaction.

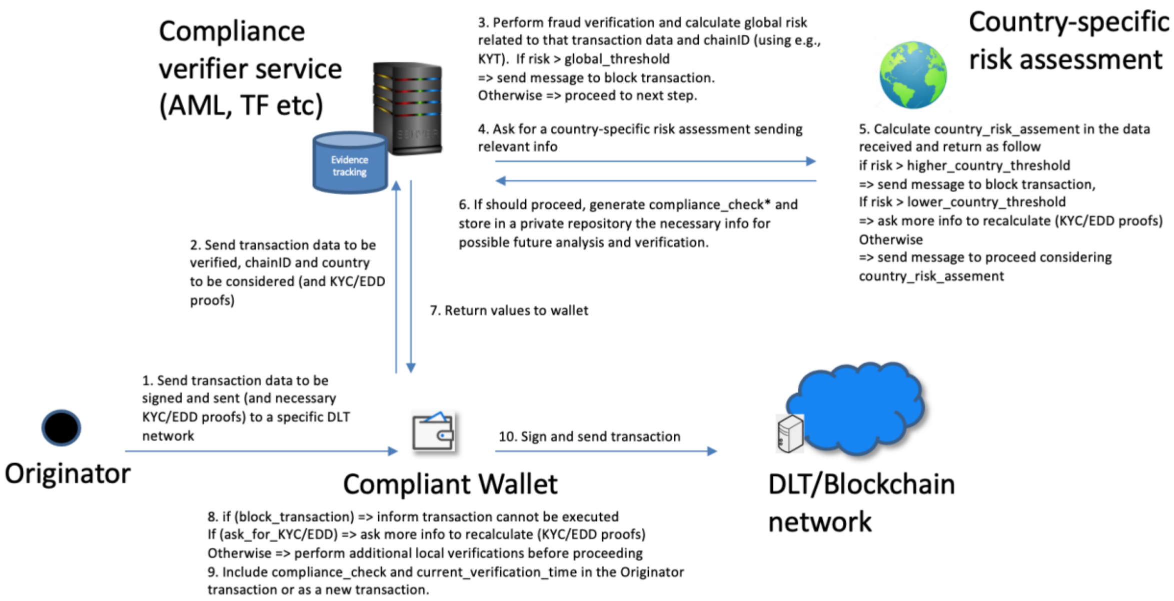
Compliance verifier service (AML, TF etc)
Evidence tracking
3. Perform fraud verification and calculate global risk related to that transaction data and chainID (using e.g., KYT). If risk > global_threshold
=> send message to block transaction.
Otherwise => proceed to next step.
Country-specific risk assessment
4. Ask for a country-specific risk assessment sending relevant info
5. Calculate country_risk_assement in the data received and return as follow
if risk > higher_country_threshold
=> send message to block transaction,
If risk > lower_country_threshold
=> ask more info to recalculate (KYC/EDD proofs)
Otherwise
=> send message to proceed considering country_risk_assement
6. If should proceed, generate compliance_check* and store in a private repository the necessary info for possible future analysis and verification.
2. Send transaction data to be verified, chainID and country to be considered (and KYC/EDD proofs)
7. Return values to wallet
1. Send transaction data to be signed and sent (and necessary KYC/EDD proofs) to a specific DLT network
Originator
10. Sign and send transaction
Compliant Wallet
DLT/Blockchain network
8. if (block_transaction) => inform transaction cannot be executed
If (ask_for_KYC/EDD) => ask more info to recalculate (KYC/EDD proofs)
Otherwise => perform additional local verifications before proceeding
9. Include compliance_check and current_verification_time in the Originator transaction or as a new transaction.

Figure 7 Overview of steps to enable KYC/AML compliance verification using compliant wallets

A compliant wallet is an application which before submitting a transaction from an Originator to the DLT/blockchain network forward it together with some additional information to be checked by a specific service, called compliance verifier service, hosted by a trusted third-party. This third-party can be private or public sector institutions and can be remunerated by doing this verification. Ideally, a compliant wallet would allow the Originator to select what verifier(s) to use in a free market.

The verification summarized in the Figure 6 may involve global analysis (for example, a KYT verification) as well as country-specific analysis. Note that it is possible to achieve a safer financial system only by doing KYT in all transactions, without any additional country-specific service. Since FATF suggests a risk-based approach (RBA) to deal with financial crimes, this guideline should be applied here. The country-level analysis may be based on traditional regulations in place or may be based on innovative ways to do KYC/AML together with a dynamic way to compute risk such as with a computational trust and risk engine (Seigneur et al., 2015) (S. Moreno & Seigneur, 2022). These innovative ways may also include privacy-preserving proofs, avoiding the disclosure of personal information in lower risk scenarios.

The result of the analysis can be codified in what Figure 6 described as compliance check, that should be signed by a private key owned by the trusted third-party and should not reveal any personal information. An additional component of this model not presented in Figure 6 is an on-chain identification of trusted third-party. This identification enables any external observer verifies that the compliance was performed correctly by a trusted third-party. Smart contracts may verify the compliance check without needing to go offchain. In this way, a new class of compliant smart contract may be created leveraging the verification of this proposal. Intermediaries, like exchanges or custodians, can also verify the compliance check and act to avoid financial crimes.

To be successful, this approach will benefit of some technical standards, including: (1) compliance level structure; (2) requirements and tests to be a compliant wallet; (3) IDs for specific DLT/blockchain networks (called chainID in the picture); (4) API of the compliance verification service; (5) KYC schemas or formats.

More information on this model can be found at the technical report "Enabling KYC and AML verification on User Transactions" (S. Moreno & Seigneur, 2022).

5 Standardization

In this section, we first discuss the standardization status for stablecoins. Then, we delve into the details of potential technical solutions for stablecoins interoperability.

The World Economic Forum and the Global Blockchain Business Council have published in 2020 a report on the blockchain technical standards being worked on in the world (*Global Standards Mapping Initiative*, 2020). They found that there has been “a proliferation of activity around technical standardization for blockchain technology” with “over 30 technical standard-setting entities, 185 jurisdictions, and nearly 400 industry groups”. However, a high volume of activity concentrated on similar topics in most groups, for example, security, identity, Internet of Things, Distributed Ledger Technology (DLT) taxonomy, ICO, KYC/AML, CBDC… Stablecoins haven’t been a topic with a high volume of standardization activity so far. They thought that there is too much fragmentation on both technical and legal standardizations aspects given that the technology is borderless and “existing efforts to coordinate among jurisdictions have been piecemeal at best and chaotic at worst”. They underlined that there are aspects of blockchains that are not yet mature enough for standardization. In the introduction of this report, we have surveyed several definitions of stablecoins and shown that stablecoins taxonomies evolve as the field of stablecoins expands. The use-cases that have been presented during the ITU online meetings covered stablecoins types such as algorithmic ones that were just a few months old. It is the reason that we have chosen to keep a simple and open definition of stablecoin, not only related to fiat pegged ones and hopefully relevant to future types of stablecoins.

Regarding stablecoin proposal processes, their report underlines that Libra created Libra improvement proposals (LIPs) similar to Bitcoin improvement proposals (BIPs) or Ethereum improvement proposals (EIPs). The problem with stablecoins, in general, is that they come from numerous independent entities from private companies all over the world to anonymous teams and traditional banks. Of course, if stablecoins would be standardized, it would help for their interoperability.

5.1 Interoperability

Still, even some existing stablecoins have demonstrated some level of interoperability. The best example of this interoperability aspect is Tether. First, it became interoperable with all ERC-20 tokens when it moved from Omni to Ethereum. ERC-20 is indeed a de facto standard invented by Ethereum to standardized the interface of coins built on Ethereum to make them more interoperable. Later on, USDT was also implemented on other blockchains such as Tron, Binance Smart Chain… as mentioned above. ERC-20 tokens are not interoperable with other blockchains. If there is a bridge between Ethereum and the other blockchain or platform then the level of interoperability increases as shown in design 1 of Figure 7.

Having a stablecoin implemented on several blockchains increases the implementation time and difficulty as well as its maintenance both from a total supply point of view split on several blockchains and technical knowledge of the different blockchains, not mentioning when security patches must be applied quickly to avoid a successful attack. In order to increase the scalability of stablecoins, they could also be implemented on layer 2 solutions. Again, in this case, their maintenance would require mastering several DLT. More recently, platforms focusing on interoperability have emerged, especially Cosmos or Polkadot. Stablecoins implemented on these platforms may then become interoperable more easily than on other independent blockchains because they do not need to build a bridge themselves as the interoperable platforms have already built-in interoperability as shown in design 2 of Figure 7. Examples of stablecoins built on interoperable platforms are the defunct Terra on Cosmos and Acala (*Acala*, n.d.) on Polkadot (*Polkadot Network*, n.d.). Polkadot is a scalable heterogeneous multi-chain blockchain, which means that it consists of a collaborative decentralized blockchain network that interacts with sharded chains running in parallel. Therefore, the interoperability of Polkadot is achieved by two main ways:

1. Internal interoperability: parallel chains are normally built with a common blockchain framework called Substrate provided by Polkadot, which allows chains to communicate in same language-cross-chain messaging (XCM) internally.

2. External interoperability: Polkadot not only deploys bridge to connect with external blockchains, but also integrate a built-in feature of the Substrate framework to call Oracle function with aim of retrieving certain type of data.

Compared with drawback of a stablecoin in Ethereum, a stablecoin in Polkadot has several advantages. Acala's aUSD, a stablecoin backed by a basket of collaterals, can freely exchange with other coins within Polkadot ecosystem, and other major crypto, like Bitcoin and Ethereum. Meanwhile, as Polkadot is able to upgrade the network without forks, new features for a stablecoin could be implemented in seconds once it is approved by on-chain governance. With aim of pegging to US dollars, aUSD will be allocated with a special messaging channel for liquidation in extreme scenarios so as to liquidate collaterals in time.

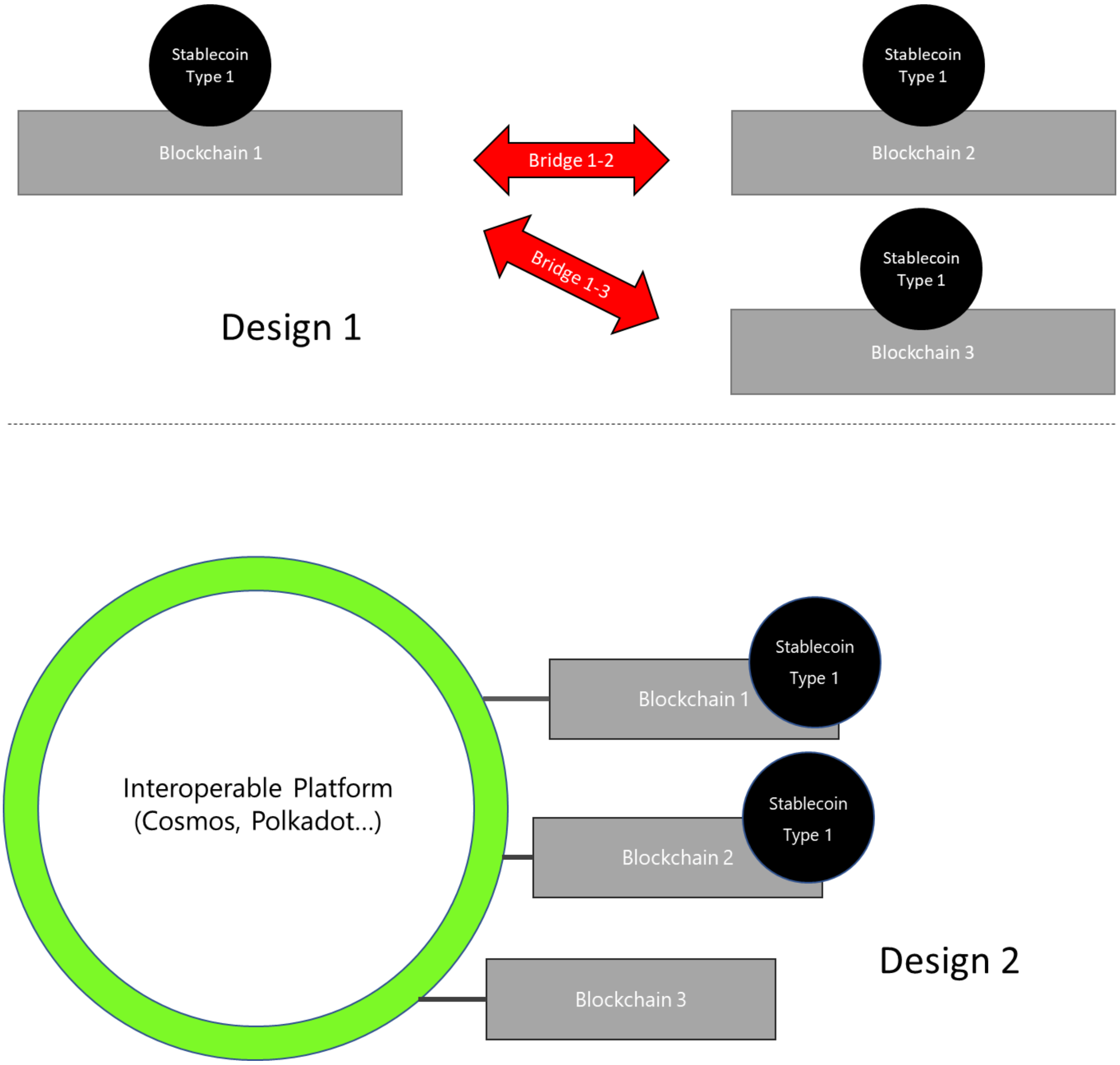

Figure 8 Stablecoins interoperability designs

5.2 Towards Legally Viable Signed NFT Standard

We have seen in section 3.5 that theoretically NFT can be considered as stablecoin when they are linked to a digital asset. However, we also underlined a few remaining practical and legal issues.

First, as the asset linked to the NFT could be lost, e.g., the Web server hosting the media linked to the NFT goes down, it seems important an NFT includes the hash of the linked digital asset. Regarding physical asset, some of hash should be also be included, e.g., the hash of an RFID chip embedded in the asset or based on recognizable (Seigneur, 2005) characteristics of the physical asset.

Second, the real identity of the address used to create the NFT could be proven thanks to a digital certificate based on qualified electronic signatures (QES) ("Qualified Electronic Signature," 2022). QES are legally viable in Switzerland and the European Union. QES are equivalent to hand-written signatures where the signing entity would have to prove the signature is invalid. The NFT could have a link to an easily readable PDF where the initial asset owner signs that she/he owns the address that has generated the NFT. Alternatively, the PDF may have a signed statement that she/he agrees that NFTs generated by this address are considered as her/his NFTs or that specific NFTs are considered as her/his NFTs. The hash of such PDF should be also included in the NFT as well as potential text version of the PDF content and digital signature as long as the size of such additional information isn’t too big to be stored in the blockchain.

Finally, the licence or conditions of the NFT should be clearly stated in the NFT as long as the size of such additional information isn’t too big to be stored in the blockchain and detailed in a linked easily PDF that would also be signed by the NFT creator, again signed with qualified level digital signature. The hash of such PDF should also be included in the NFT. In the digital art domain, the licence would list the rights given to the buyer, the rights retained by the artist, the number of potential copies, the secondary sales royalty percentage… A reference implementation of such approach has been started as part of the ArtistCert service (*ArtistCert*, n.d.). Further privacy considerations will have to be considered in the case of non-public entities.

6 Conclusion

We have seen that the realm of stablecoins is quite diverse and still expanding. Stablecoins aiming to be stable with regards to fiat currency aren’t the only types of stablecoins. For example, we have covered a stablecoin aiming to be stable with regards to purchasing power. The definition that we have provided in the introduction seems generic enough to cope with their diversity and future types.

Another important point is that there are major legal aspects that must be taken into account, which is not always the case for technologies. Furthermore, if the stablecoins are aimed at working on an international scale then compliance becomes even more difficult given all the different legal approaches in the world.

Recommendation 1: In order to achieve a broad range of compliance requirements, stablecoins should go through compliant crypto-wallets that are able to carry out compliance checks before any transaction, for example, either thanks to a compliance proofs third-party service or a computational trust and risk engine embedded directly in the crypto-wallet.

Recommendation 2: Whilst financial compliance is mandatory, privacy protection when using stablecoins should be sought after too.

Stablecoins technical interoperability is still also in its infancy because platforms for interoperable blockchains such as Cosmos or Polkadot are just being launched on mainnets, i.e., in real settings. Nevertheless, a stablecoin implemented on an interoperable platform such as Cosmos or Polkadot is less difficult to bridge to other blockchains because the bridges already exist.

Recommendation 3: To facilitate their interoperability, stablecoins should be implemented on interoperable platforms such as Polkadot or Cosmos.

Stablecoins backed by fiat money have gained most of the attention by the regulators due to their impact on the financial market and the risks that retail investors or users if they weren’t fully backed or badly implemented. The security working group of our digital currency global initiative (DCGI) will be useful to try to standardize how audits should be done for these projects and how to evaluate the security of these projects. However, given the recent major issues on existing algorithmic stablecoins and on the real reserve of existing reserved-based stablecoins such USDT, CBDC would provide safer solutions in this regard because there is no trust issue in the reserve or algorithm as the CBDC is created by the central bank, which creates the fiat currency. Since the first version of this technical report, major stablecoins pegged to the $ have lost their peg either to a small degree like USDT, which may really depegged in the future due to several risks (reserve risk, US government cease and desist order…), or UST that completely depegged and crashed to almost 0. More work is needed both at the technical level and at the social level to help people not being fooled by untrustworthy projects.

7 Bibliography

Acala. (n.d.). Retrieved June 20, 2022, from https://acala.network/

Arner, D., Auer, R., & Frost, J. (2020). *Stablecoins: Potential, risks and regulation* (BIS Working Paper No. 905). Bank for International Settlements. https://econpapers.repec.org/paper/bisbiswps/905.htm

ArtistCert. (n.d.). Retrieved June 24, 2022, from https://www.artistcert.art/

Bharathan, V. (2021). *People's Bank Of China Draft Law Provides A Legal Basis For Digital Currency Electronic Payments (DC/EP) And Bans All Stablecoins Backed By Renminbi Reserves*. Forbes. https://www.forbes.com/sites/vipinbharathan/2020/10/24/peoples-bank-of-china-draft-law-provides-a-legal-basis-for-digital-currency-electronic-payments-dcep-and-bans-all-stablecoins-backed-by-renminbi-reserves/

Bhat, S., Kahya, A., Kumar, R., & Krishnamachari, B. (2021). Simulating the MakerDAO Stablecoin. *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 1–2.

Bolliger, C. (2019). *Stablecoins—Classification of stablecoins and their impact on the financial sector*.

Boltshauser, T., & Seigneur, J.-M. (2021a). *Libra / Diem Stablecoin Use-Case* (DCGI-AIRU-I-052; Digital Currency Global Initiative). ITU.

Boltshauser, T., & Seigneur, J.-M. (2021b). *USDT Stablecoin Use-Case* (DCGI-AIRU-I-051; Digital Currency Global Initiative). ITU.

Bullmann, D., Klemm, J., & Pinna, A. (2019). *In Search for Stability in Crypto-Assets: Are Stablecoins the Solution?* (SSRN Scholarly Paper ID 3444847). Social Science Research Network. https://papers.ssrn.com/abstract=3444847

Congresswoman Rashida Tlaib sur Twitter. (2020). Twitter. https://twitter.com/RepRashida/status/1334247450731819008

Copic, E. (2020). *Celo Stablecoin Use-Case* (DCGI-AIRU-I-020; Digital Currency Global Initiative). ITU.

Cox, J. (2021, May 21). *Bitcoin price falls after China calls for crackdown on bitcoin mining and trading behavior*. CNBC. https://www.cnbc.com/2021/05/21/bitcoin-falls-after-china-calls-for-crackdown-on-bitcoin-mining-and-trading-behavior.html

Dalton, M. (2022, August 17). Acala Has Recovered Almost 3B aUSD. *Crypto Briefing*. https://cryptobriefing.com/acala-has-recovered-almost-3b-ausd/

Entriken, W., Shirley, D., Evans, J., & Sachs, N. (2018). *ERC-721 Non-Fungible Token Standard*. Ethereum.Org. https://ethereum.org

FATF-GAFI - Financial Action Task Force. (n.d.). Retrieved February 24, 2020, from https://www.fatf-gafi.org/

Federal Council brings DLT Act fully into force and issues ordinance. (2021). https://www.admin.ch/gov/en/start/documentation/media-releases/media-releases-federal-council.msg-id-84035.html

FINMA publishes 'stable coin' guidelines. (2019). Eidgenössische Finanzmarktaufsicht FINMA. https://www.finma.ch:443/en/news/2019/09/20190911-mm-stable-coins/

FSB consults on regulatory, supervisory and oversight recommendations for "global stablecoin" arrangements. (2020, April 14). https://www.fsb.org/2020/04/fsb-consults-on-regulatory-supervisory-and-oversight-recommendations-for-global-stablecoin-arrangements/

Global Standards Mapping Initiative: An overview of blockchain technical standards. (2020). World Economic Forum. https://www.weforum.org/whitepapers/global-standards-mapping-initiative-an-overview-of-blockchain-technical-standards/

Haeberli, D., Oesterhelt, S., & Wherlock, A. (2021). *Blockchain & Cryptocurrency Laws and Regulations | Switzerland | GLI* (United Kingdom) [Text]. GLI - Global Legal Insights - International Legal Business Solutions; Global Legal Group.

https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/switzerland

IPFS Powers the Distributed Web. (n.d.). Retrieved June 23, 2022, from https://ipfs.io/

J.P. Morgan Creates Digital Coin for Payments. (2019). https://www.jpmorgan.com/solutions/cib/news/digital-coin-payments

La FINMA publie un guide pratique sur les ICO. (2018). Eidgenössische Finanzmarktaufsicht FINMA. https://www.finma.ch:443/fr/news/2018/02/20180216-mm-ico-wegleitung/

Lartigau, J. (2021). *Lugh Stablecoin Use-Case* (DCGI-AIRU-I-062; Digital Currency Global Initiative). ITU.

Lipton, A., Sardon, A., Schär, F., & Schüpbach, C. (2020). *From Tether to Libra: Stablecoins, Digital Currency and the Future of Money*.

Loon, L. Y. (2021). *Decentralized Stablecoins: An Unfulfilled Promise?* https://www.nansen.ai//research/decentralized-stablecoins-an-unfulfilled-promise

Moin, A., Sirer, E. G., & Sekniqi, K. (2019). A Classification Framework for Stablecoin Designs. *ArXiv:1910.10098 [Cs, q-Fin]*. http://arxiv.org/abs/1910.10098

Moreno, S. M. B. M., & Almeida, V. (2020). *BNDES Stablecoin Use-Case* (DCGI-AIRU-I-021-R1; Digital Currency Global Initiative). ITU.

Moreno, S. M. B. M., Seigneur, J.-M., & Gotzev, G. (2021). *A Survey of KYC/AML for Cryptocurrencies Transactions* [Chapter]. Handbook of Research on Cyber Crime and Information Privacy; IGI Global. https://doi.org/10.4018/978-1-7998-5728-0.ch002

Moreno, S., & Seigneur, J.-M. (2022). *Enabling KYC and AML verification on User Transactions* [Technical Report]. University of Geneva.

Notabene. (2022). *State of Crypto Travel Rule Compliance Report 2022*. https://notabene.id/state-of-crypto-travel-rule-compliance-report

Open Vasp – An Open Protocol to Implement FATF’s Travel Rule for Virtual Assets. (n.d.). Retrieved March 15, 2020, from https://www.openvasp.org/

Polkadot Network. (n.d.). Polkadot Network. Retrieved June 20, 2022, from https://polkadot.network/

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a pilot regime for market infrastructures based on distributed ledger technology, (2020). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0594

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-assets. (2020). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593

Qualified electronic signature. (2022). In *Wikipedia*. https://en.wikipedia.org/w/index.php?title=Qualified_electronic_signature&oldid=1094665120

Sam Bankman-Fried breaks down how the crypto tax provision in the infrastructure bill could force swaths of the industry out of the US | Currency News | Financial and Business News | Markets Insider. (2021). https://markets.businessinsider.com/news/currencies/sam-bankman-fried-crypto-tax-provision-industry-offshore-infrastructure-bill-2021-8

Seigneur, J.-M. (2005). *Trust, Security and Privacy in Global Computing*. Trinity College Dublin. https://www.cs.tcd.ie/publications/tech-reports/reports.06/TCD-CS-2006-02.pdf

Seigneur, J.-M. (2019). *Secure transaction system between terminals* (Patent No. FR3077151A1). https://patents.google.com/patent/FR3077151A1/en

Seigneur, J.-M. (2020). *GLX Stablecoin Use-Case* (DCGI-AIRU-I-019; Digital Currency Global Initiative). ITU.

Seigneur, J.-M., Ballester Lafuente, C., Titi, X., & Guislain, J. (2015). OPPRIM: Opportunity-enabled risk management for trust and risk-aware asset access decision-making. *University of Geneva Technical Report*.

Seigneur, J.-M., D'Hautefort, H., & Ballocchi, G. (2017). *Use case of linking a managed basket of fiat currencies to crypto-tokens*. First Meeting of the ITU Focus Group on Digital Currency including Digital Fiat Currency. https://archive-ouverte.unige.ch/unige:97657

Shin, H. S. (2022). *III. The future monetary system*. https://www.bis.org/publ/arpdf/ar2022e3.htm

Tan, L., & Seigneur, J.-M. (2020a). *Ampleforth Stablecoin Use-Case* (DCGI-AIRU-I-022; Digital Currency Global Initiative). ITU.

Tan, L., & Seigneur, J.-M. (2020b). *DAI Stablecoin Use-Case* (DCGI-AIRU-I-018; Digital Currency Global Initiative). ITU.

Three Schemes for Dual Offline Payment of CBDC, Says China's Central Bank | NEWS.8BTC.COM. (2020). https://news.8btc.com/three-schemes-for-dual-offline-payment-of-cbdc-says-chinas-central-bank

Tlaib, García and Lynch Introduce Legislation Protecting Consumers from Cryptocurrency-Related Financial Threats. (2020, December 2). Representative Rashida Tlaib. https://tlaib.house.gov/media/press-releases/tlaib-garcia-and-lynch-stableact

Trisa.io Travel Rule Compliance – FATF guidance. (n.d.). Retrieved March 15, 2020, from https://trisa.io/

Yaffe-Bellany, D., & Griffith, E. (2022, May 18). How a Trash-Talking Crypto Founder Caused a $40 Billion Crash. *The New York Times*. https://www.nytimes.com/2022/05/18/technology/terra-luna-cryptocurrency-do-kwon.html

Zhang, G. (2022). *A-USD Acala Polkadot* (DCGI-AIRU-I-092; Digital Currency Global Initiative). ITU.

Zhao, W. (2021). *China's Inner Mongolia set to impose eight measures on crypto mining ban*. https://www.theblockcrypto.com/post/105973/china-inner-mongolia-crypto-bitcoin-mining-ban-measures