BANK OF CANADA
BANQUE DU CANADA

Staff Discussion Paper/Document d'analyse du personnel — 2021-6

Last updated: April 8, 2021

Stablecoin Assessment Framework

by Alejandro Garcia, Bena Lands and Dennis Yanchus

Financial Stability Department
Bank of Canada, Ottawa, Ontario, Canada K1A 0G9

AGarcia@bank-banque-canada.ca, BLands@bank-banque-canada.ca, and DYanchus@bank-banque-canada.ca

ISSN 1914-0568

Acknowledgements

We thank Scott Hendry, Francisco Rivadeneyra, Cyrus Minwalla and Alexandra Lai for valuable comments.

Abstract

We outline a three-step framework to investigate stablecoin arrangements and quantitatively assess their risk. The first step is to classify the stablecoin arrangement into three parts—coin structure, transfer system(s) and financial service(s)—and categorize the attributes of each part. The second step is to identify specific risk scenarios. The third is to quantify the range of probable loss and range of possible frequency associated with the identified risk scenarios. Our proposed framework allows authorities to understand the defining characteristics of stablecoin arrangements, to be specific about any concerns they may have, and to be objective in their treatment from issuer to issuer. Additionally, the process we are proposing ensures that authorities and the stablecoin issuer can come to a quantitatively based understanding about the potential risks. The main contributions we make are to separate stablecoins arrangements into three activity-based components and to apply an operational risk management approach to quantifying risks of stablecoins.

Topics: Digital currencies and fintech; financial institutions; Financial system regulation and policies; Financial markets; Payment clearing and settlement systems
JEL codes: D78, D81, G01, G18, O3, O38

Introduction

The creation of a cryptocurrency[1] includes formalizing a network of actors and technologies—an arrangement—that includes links to new or existing payment and financial service providers. Many types of these arrangements exist, and they all have the potential to be widely used as a means of payment or store of value. They include cryptocurrencies with a price stabilization mechanism, such as Tether, or those without, such as Bitcoin or Ether.[2]

Our focus in this paper is on cryptocurrencies that attempt to maintain price stability with an existing national currency—so-called stablecoins—but our work applies to all cryptocurrencies. Although stablecoins make up a small share of the cryptocurrency market, they have the potential to improve the supply and scope of financial services. However, depending on their design and evolution, this efficiency could come with significant risk to financial stability.

Given the novelty of stablecoins, no universal assessment framework exists. This makes it unclear how to evaluate the benefits and risks of stablecoin arrangements. The challenge is to ensure that stablecoin issuers[3] make risk management decisions that are in line with what regulators expect from equivalent transfer systems and financial services providers. As with other financial innovations, relevant authorities need to understand the financial and operational risks that come with increased use of stablecoins—and cryptocurrencies more broadly. Only then can they manage the potential negative effects on the financial system and the economy. A guiding principle that has gained some popularity with authorities is the idea of "same business, same risks, same rules."[4] A more appropriate principle may be "same business, same risks, *equivalent* rules," as there may be different risks depending on the technological choices and service providers. The principle of equivalent rules—rules that differ but result in the same risk controls—may be a better way to address the risks of stablecoin arrangements.

In this paper, we propose a three-step process to categorize and assess the risks associated with stablecoin arrangements.

---

[1] We use the term cryptocurrency here in the sense given to "virtual currency" by the US Department of the Treasury: "a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency," the most important being legal tender status (Financial Crimes Enforcement Network 2013).

[2] Some have argued that Bitcoin can never be money (Bailey 2020); however, many factors can drive adoption of a cryptocurrency. Existing cryptocurrencies can also become more liquid, more accepted and eventually stable enough to significantly compete with fiat money (Chambers 2019; McBride 2020). Using our proposed assessment framework will help authorities identify the cryptocurrencies to watch, whether stable or otherwise.

[3] We use "stablecoin arrangement" when referring to the system and "stablecoin issuer" when referring to the system's operator.

[4] See Financial Stability Board (2020), Lautenschläger (2019), Restoy (2019) and Hubert (2016) for the wider policy discussion.

The first step is a categorization exercise that allows the relevant authority to understand the defining characteristics of the stablecoin arrangement, identify red flags and compare it with other arrangements.[5] To this end, we categorize the stablecoin arrangement into three parts—the coin structure, the related transfer system and the related financial service—and then break down each of these parts into multiple subcategories. Separating the activities of the arrangement into standalone parts ensures that we clearly identify all the functions, processes and actors, along with their associated risks.

The second step is to identify specific risk scenarios presented by the stablecoin arrangement. These need to be well-defined to quantify their potential impact. Therefore, when identifying specific risks, we must articulate a time horizon for the risk event, the asset at risk and a precise description of the risk scenario.

The third and final step is to quantify the range of probable loss and the range of probable frequency associated with the specific risk scenarios identified. Our approach draws on the Factor Analysis of Information Risk (FAIR) model,[6] which provides a quantifiable and reproducible way of estimating the loss event frequency and loss magnitude of various risk scenarios (see Freund and Jones 2015). Without such an approach, it is difficult to assess whether the stablecoin issuer is managing its risk prudently, demonstrating its compliance and effectively communicating risk mitigation strategies to internal and external stakeholders.

Our use of the FAIR model is novel in two ways:

1. We propose to use the model from the outside looking in and as the basis for a conversation between an authority and the stablecoin issuer rather than as a framework for the institution to apply internally to quantify risks.
2. We propose to expand the losses quantified to include both those internalized by the issuer and those not in keeping with the goals of financial stability.

Using this framework to evaluate stablecoin arrangements will allow authorities to understand their characteristics, quantify risks and gather evidence that firms are effectively allocating risk management resources. Once this framework is in place, authorities can more easily perform ongoing monitoring and updating.

The remainder of this paper is organized as follows: we first provide a high-level overview of what stablecoins are, we then walk through the three steps of the framework and we conclude with some final remarks.

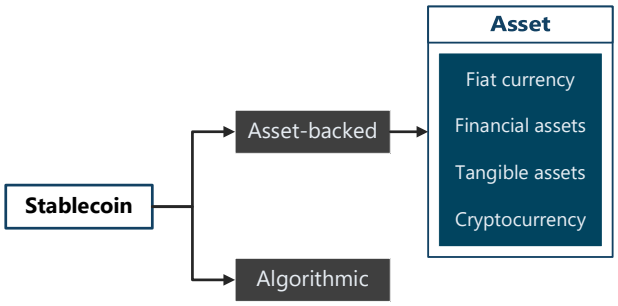
[5] To facilitate the use of the framework for step one, we plan to distribute an electronic survey that can be used to streamline the process to categorize the stablecoins.

[6] The FAIR model is used by hundreds of companies—including a number of large US banks and US government agencies—to conduct their quantitative risk analysis.

What are stablecoins?

Stablecoins are a type of cryptocurrency that uses a stabilization mechanism to attempt to maintain price stability with an existing national currency or other asset.[7] Stablecoin arrangements refer to a range of functions and related activities that provide a means of payment or store of value, or both.[8] Although the term "stablecoin" implies fixed convertibility to some currency or other asset, this may not always be the case. Most stablecoins try to maintain stability by tying their value to a reference asset, linking to the reference asset through an asset-backed mechanism or algorithm (**Figure 1**).[9] The stabilization mechanism is just one part of the stablecoin arrangement. Identifying and categorizing the other parts of the arrangement are also important to understand all the risks. Step one, described below, illustrates our approach.

Figure 1: Stabilization mechanisms



Step 1. Categorization—understanding the arrangement

Step one organizes the stablecoin arrangement into three different parts, focusing on:

1. coin structure
2. transfer of the coin between users
3. financial services accessed using the coin

[7] Most stablecoins are actually tokens, not coins. In other words, they do not have their own blockchain and are built on an existing blockchain(s). Bitcoin, Ethereum and Tron are some of the most popular. We use the term "coin" throughout to discuss both coins and tokens.

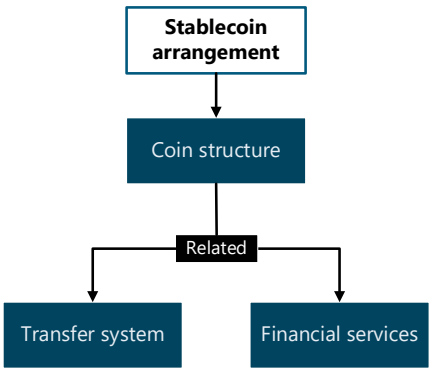
[8] A more detailed definition is available from the President's Working Group on Financial Markets (2020, 1), which states that a stablecoin arrangement includes "the stablecoin as well as infrastructure and entities involved in developing, offering, trading, administering or redeeming the stablecoin, including, but not limited to, issuers, custodians, auditors, market makers, liquidity providers, managers, wallet providers, and governance structures."

[9] Algorithmic stabilization mechanisms use an algorithm to manage the supply of the coin, consequently controlling its price. They are not backed by any existing assets, off or on chain. The stability relies on the confidence of the coin holder in the stablecoin arrangement, including the smart contract rules that determine supply and incentives for coin holders.

Not all coins have related transfer systems or financial services.

Taking this approach allows the relevant authority to match up the attributes of the stablecoin arrangement with traditional currency and bank money arrangements (see **Figure 2**).

Figure 2: Categorization of stablecoin arrangements



We divide the three parts of a stablecoin arrangement—coin structure, transfer system and financial service—further into three broad categories, which we present in three shades in the figures that follow:

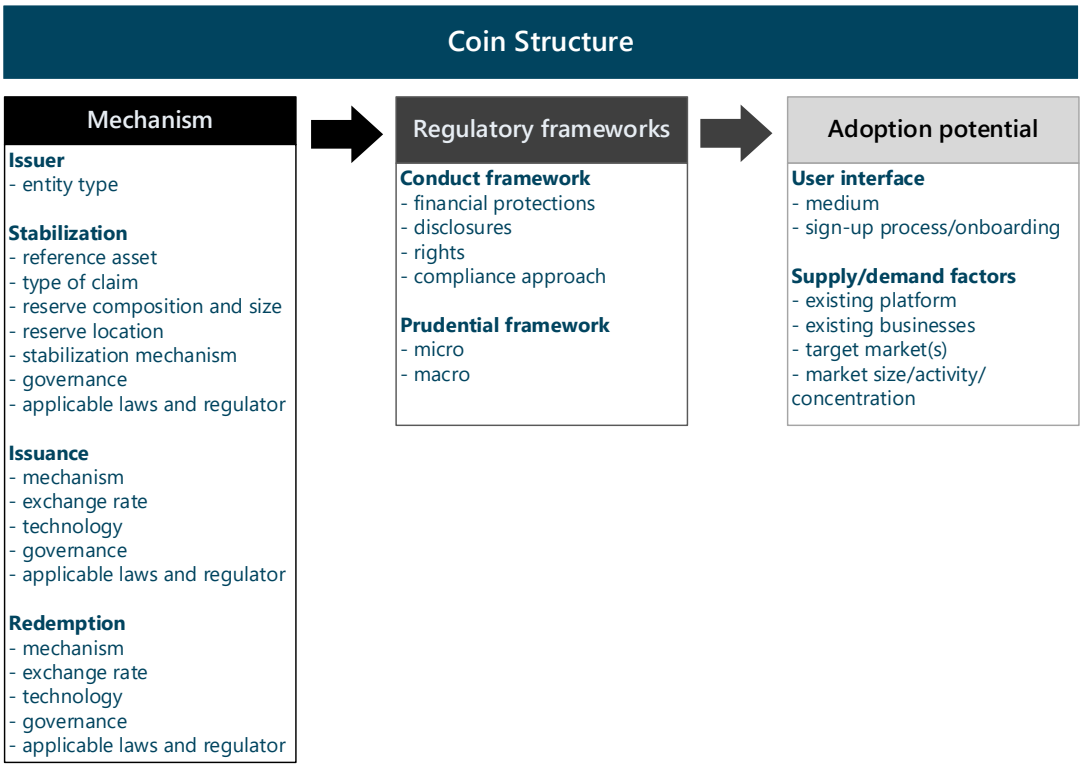
- the mechanics of the coin, system or service (black)
- any regulatory frameworks that apply (dark grey)
- the potential drivers of adoption (light grey)

Defining the attributes in these broad three categories will ensure a full understanding of the stablecoin arrangement, including the risks, liabilities and incentive interactions between issuer, transfer system and financial service provider. The boxes in dark blue in Figures 3, 4 and 5 must be populated with the pertinent information for a relevant authority to fully understand each part of the arrangement

The coin structure

The first step in assessing a stablecoin arrangement is to define the coin's structure (see **Figure 3**, and see Appendix A for complete categorization).

Figure 3: **Categorization of the coin structure**



Mechanics

In identifying the mechanics of the coin, we start with the *issuer type*. Identifying the issuer type helps clarify whether, where and how the entity is regulated. For example, if the issuer is a deposit-taking institution (e.g., a bank), it will already have designated regulators and be subject to multiple banking and financial regulations. Issuer type can also suggest the motivations for launching the stablecoin arrangement—that is, for profit, strategic positioning or sovereignty.[10]

Next in the mechanics category is the coin's *stabilization* method, including the reference asset, reserve assets, composition and location, stabilization mechanism, governance and applicable laws. Understanding stabilization—that is, how the issuer maintains the peg to the reference asset—is particularly important. For example, is stabilization maintained similarly to an exchange traded fund, through the arbitrage trading of a few large institutional entities? Or does it occur through a mechanism of smart contracts? Also important are the governance and the laws applicable to the stabilization mechanism. Is there an internal policy, or are applicable laws for custody or segregation of reserve assets in place?

[10] For example, in the case of a central bank digital currency, sovereignty is often an important driver for issuance.

Finally in the mechanics category are *issuance* and *redemption*.[11] These are separated because the actors, rules and mechanisms involved in issuing the coin can differ from those in redeeming the coin. For both issuance and redemption, we describe the specific mechanisms, exchange rate policy and underlying technologies.

The exchange rate policy is important for understanding how the coin may function in both normal and stressed market conditions. The issuer could stand ready to exchange the coin one-to-one for fiat currency (e.g., the US dollar) less fees at all times or only in some limited circumstances. For redemption, it should be clear when and if the coin is redeemable and for what asset and value. Can the issuer apply different fees or deliver different assets in normal versus stressed market conditions? Not all coins are explicitly redeemable for the reference or reserve assets, and many impose fees or restrictions during stress events. These details should be clearly noted, as they could affect liquidity and result in the price of the coin deviating from the reference asset.

Once redemption has been well defined, the categorization exercise shifts focus from the mechanisms to the regulatory frameworks, if any exist.

Regulatory frameworks

We assess two types of regulatory framework: those that address *conduct* and those that address *micro- and macroprudential regulation*.[12]

Assessing conduct regulation includes identifying any risk or information disclosures, such as prospectuses, applicable user rights (e.g., rights of rescission), complaint handling and financial protections. Identifying know-your-client (KYC), know-your-product (KYP) and suitability requirements is also important. In many cases, authorities will be identifying what is missing or the lack of equivalent conduct regulation.

Similarly, in assessing the prudential framework, both micro and macro, authorities will be looking for any capital and liquidity requirements that apply, as well as backstops, such as lender of last resort and recovery and resolution arrangements. Once again, authorities will be looking for equivalent prudential regulation for offerings and in many cases noting its absence.

Potential drivers of adoption

Two subcategories aid in understanding the potential for adoption. These are *user interface* and *supply and demand factors*.

---

[11] Issuance is a description of the coin's primary distribution as opposed to secondary distribution, in which existing coins are transferred between the buyers and sellers. Secondary trading is captured in the analysis of the transfer system. Redemption is the process by which coins are "destroyed." This is similar to the process by which exchange traded funds or other mutual fund shares/units are redeemed directly by the fund manager, as opposed to being sold to other investors in the secondary market.

[12] Most stablecoin arrangements in existence today have limited regulatory frameworks in place. Regulation could be in the form of self-regulatory activity or more formal government regulation.

The user interface subcategory shows how and which users are meant to access the initial distribution. Issuers that require high account minimums and fees will ensure that only large market players access the primary market. Other issuers may want to encourage retail access to the primary market by offering low minimums or a mobile app with friendly user interface and an intuitive sign-up process. The setup of the issuer's user interface may raise compliance issues, especially those around anti-money-laundering (AML) requirements.

Regarding the supply and demand factors subcategory, the arrangement's capability to drive demand and provide supply will depend in part on whether it has pre-existing platforms or businesses to easily distribute its stablecoin. For example, a large social media company will already have a meaningful online consumer base to which it can promote its stablecoin. This promotion could include integrating the stablecoin into its existing services. An online brokerage firm, in contrast, could offer a stablecoin to its clients through its existing platform as a new investment product or way to hold foreign currency. These are just two examples of how organizations with existing clients and services can use them to create demand and enable supply.

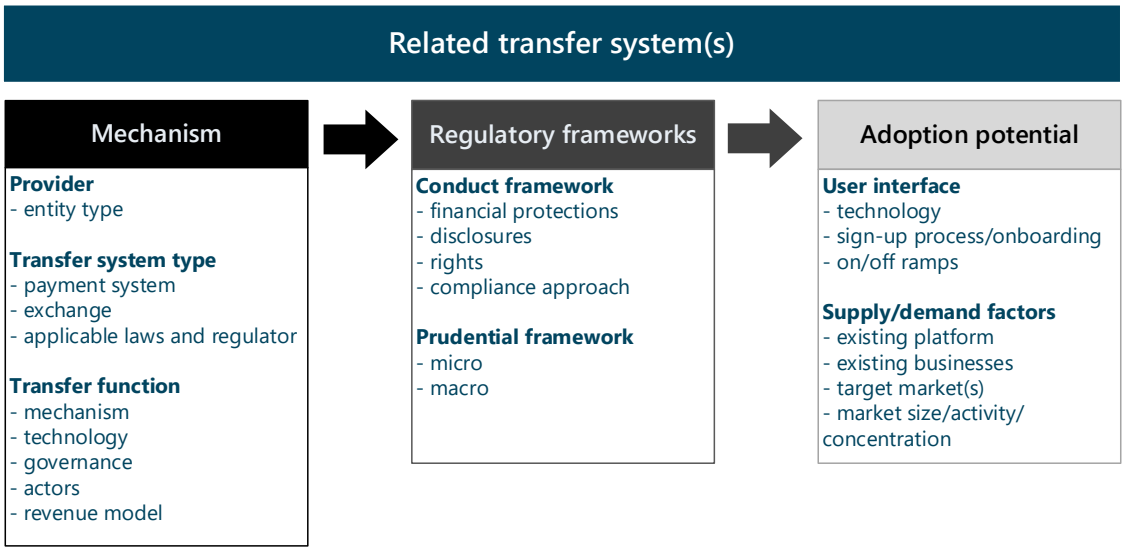
Adoption can also be driven by the target market of the arrangement. A clearly defined target market can inform the business case, including the revenue model. It may also highlight certain economic risks the arrangement could create. As an example, assume there is a stablecoin arrangement that targets individuals in high inflation countries by offering a stablecoin that is pegged to a basket of the three most stable fiat currencies. The target market may be smaller than a market that targets all smartphone users, but it may be more incentivized.

Authorities should also monitor activity, taking stock of such information as the coin's market capitalization, trading volume and concentration to assess its current or potential importance. For instance, tracking a coin's market capitalization and growth rate may help identify whether the coin poses current or possible future financial stability risks.

The transfer system

Related transfer or payment systems are those that are operated directly by one of the parties that perform the stabilization, issuance or redemption of the stablecoin arrangement (see **Figure 4**, and see Appendix B for complete categorization). The categorization exercise for the transfer system follows the same structure as in Figure 3. This exercise can also be performed independently of the coin structure analysis in situations where the focus is on a particular stablecoin payment or transfer system under the arrangement.

Figure 4: Categorization of the related transfer system



Mechanics

The exercise starts with identifying the mechanics of the transfer system. First is the *provider type*—that is, the type of institution backing the activity. This is often, but not necessarily, the same as issuer type in the coin exercise.

Next, we identify the *transfer system type*—in other words, the activity being offered. If the service is related to payments, the exact type of payment offered needs to be clearly explained. Is the service focused on wholesale or retail, domestic or international payments? Understanding the service offering will help us to identify the applicable laws, regulations and regulatory authorities.

The final subcategory of the mechanics of the transfer system is the *transfer function*, which includes the mechanism, technology and revenue model. This part of the exercise will help us understand how much of the function is taking place on or off chain and the types of actors and risks involved. For instance, if the entire system resides on chain, the risks will come predominantly from the technological infrastructure and code vulnerabilities.

Regulatory frameworks

The *regulatory frameworks* assessed for the transfer system are the same as those for the coin: frameworks for conduct and for micro- and macroprudential regulation. However, these are adapted based on the type of service being performed. For example, the type of conduct framework applied to a marketplace or exchange will differ from that of a payment system.

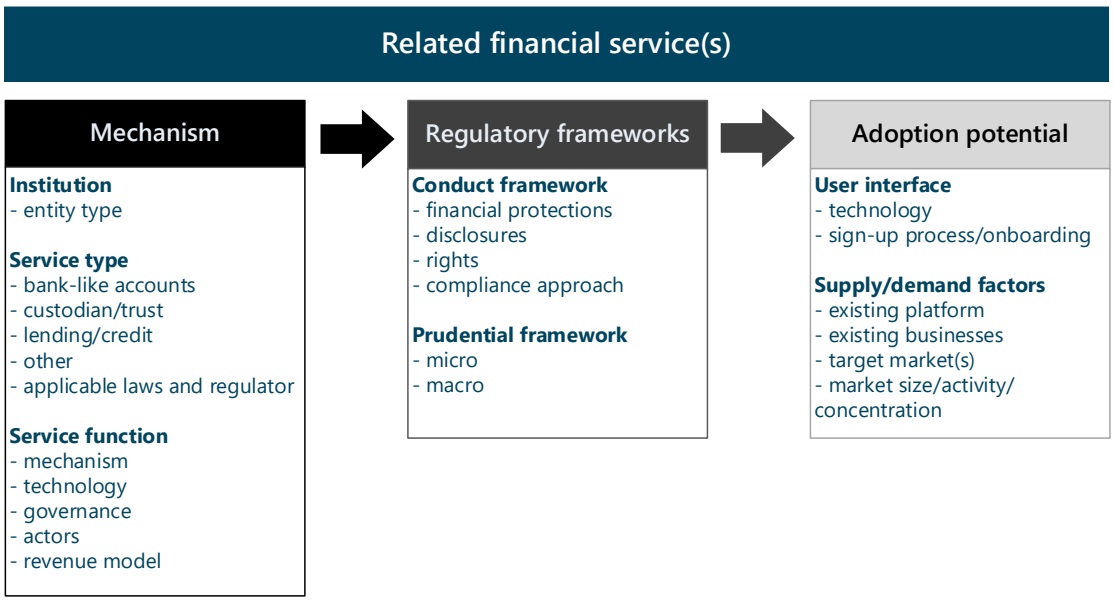
Potential drivers of adoption

The final category, as before, identifies potential drivers of adoption by calling out *supply and demand factors*, such as any affiliated businesses (e.g., an existing payment service), and *user interface* features. For instance, if a bank creates a coin and an affiliated transfer system, both the coin and the transfer service could be quickly adopted because the bank's current customers already use it for transfer services. From the customer's perspective, the stablecoin arrangement simply represents a new service offering from a trusted service provider, which makes it comparatively more attractive than an unknown transfer service provider.

Financial services

We perform a similar exercise as the above for any financial services related to the coin (see **Figure 5**, and see Appendix C for complete categorization). Such a service provider could be, for example, a related entity that offers lending using the issuer's coin. The financial service could be the primary revenue-generating activity, with the coin acting solely as a medium to provide the service. It is therefore important to understand what these services are and whether they present any risks.

Figure 5: Categorization of the related financial services



Mechanics

The exercise starts again with identifying mechanics—here, of services. We begin with the *type of institution* offering the service, which may or may not be the same as the coin or transfer system provider. Then we define the *service* and its applicable laws.

Regulatory frameworks

This is followed by the regulatory frameworks as described above—that is, for *conduct* and for *micro- and macroprudential regulation*. Financial services are heavily regulated, and therefore

it is essential that we identify the services and their applicable regulations, laws and risk controls. For banking, this includes at the minimum capital and liquidity requirements.

Potential drivers of adoption

Finally, we describe the *supply and demand factors* that could drive adoption. An example could be an online brokerage firm that offers derivatives for its coin and other stablecoins. The firm already has a platform, customers and expertise in financial products. As a result, the online brokerage's coin and related derivative products could have a sizeable market share in a short period of time.

This last step completes the categorization exercise and the first step of the assessment. Some of the specific risks of the arrangement should become apparent through the categorization exercise, while others will be identified in the next step. In any case, at this point, authorities can summarize the red flags uncovered and items that need further investigation.

Step 2: Scoping risk—identifying specific scenarios

Having categorized the stablecoin arrangement, we proceed to identify specific risk scenarios. Step two is about transforming general concerns into specific, well-defined risk scenarios that can be used as the basis for quantitative discussions between authorities and stablecoin issuers.[13] The analysis conducted in step one will likely result in several concerns that can be transformed into such scenarios in this step.[14]

Specific, well-defined risk scenarios clearly identify the asset at risk, the threat actor, the effect on the asset and the time period in which the risk is being considered. The scenario can also specify the method or methods used to impact the asset (e.g., distributed denial of service [DDoS], copying data via USB).[15]

Based on the international policy discussion on stablecoins, we have identified the main threat actors, assets and effects that apply to stablecoin arrangements (see **Figure 6**).[16] These are the building blocks that can be used by authorities to build specific risk scenarios.

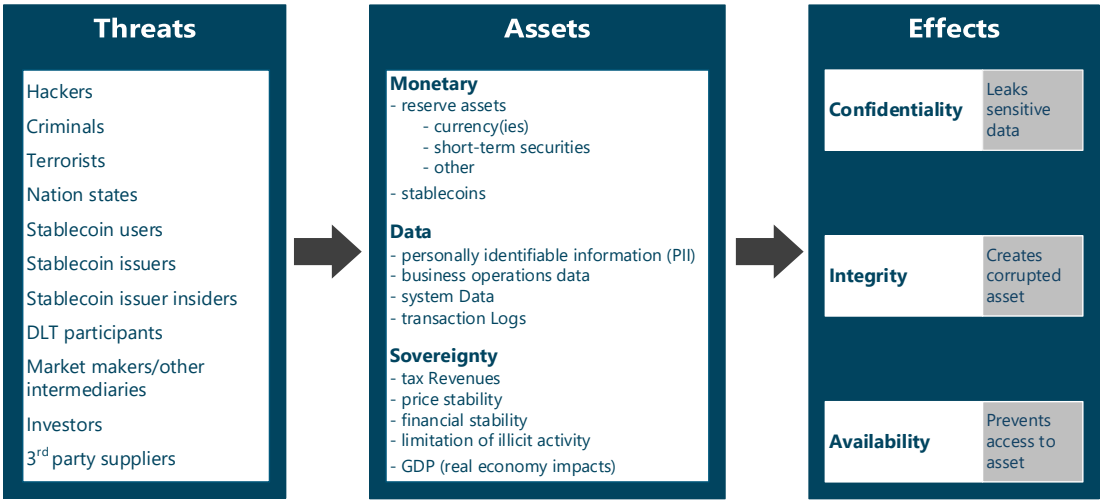
[13] For steps two and three, we apply the FAIR framework or slight modifications of it. More information on this model can be found on the FAIR Institute website.

[14] Authorities will likely have other concerns (e.g., about monetary sovereignty, cyber security or privacy risks) that can also be transformed into specific risk scenarios in this step.

[15] Most risk discussions—particularly ones focused on events in real time, where the threat actor and effects may not be known—focus on methods. However, our focus here is on quantifying exposure, risk minimization and effective resource allocation, which is impossible to do if the asset, threat and effect are left undefined.

[16] See, for example, the work by the G7 Working Group on Stablecoins (2019) and Financial Stability Board (2020).

Figure 6: Key threats, assets and effects of stablecoins



Threats

Threats are individuals, entities or "things" that act on an asset, such as criminals, stablecoin users or tornados. They are not methods of attack, like forging signatures or hacking techniques, and they are not technologies that may be used for good or ill, such as artificial intelligence.

Assets

We identify three high-level assets at risk in stablecoin arrangements: *monetary*, *data* and *sovereignty*. Monetary assets include the stablecoin and the reserve assets held against it. Data assets include personally identifiable information (PII), operational data and other valuable data generated by the stablecoin arrangement. The assets of sovereignty include public good and self-determination "assets," such as the ability to tax, maintain financial stability and sustain economic activity.

Effects

Next, we turn to the effect the threat has on the asset. Assets can be affected in three ways: their *confidentiality* can be compromised, their *integrity* can be lost or their *availability* can be reduced (e.g., through theft).[17] As with the other elements of the risk scenario, specifying the effect ensures agreement among those helping to quantify it. For example, the total amount and the types of losses that result from the release of PII (confidentiality) are much different from those that result from the corruption of PII (integrity).

Once the set of assets, threats and effects has been identified, authorities or issuers can conduct a scoping exercise using a table that lays out all the permutations to identify those scenarios that combine high value assets with significant threats (see Appendix D). While

[17] Confidentiality is affected when the threat causes loss by disclosing something about the asset. Integrity is affected when the threat causes loss by impacting the accuracy or reliability of the asset. Availability is affected when the threat causes loss by reducing access to the asset.

many permutations are possible, only a subset will result in realistic scenarios based on the known motivations and capabilities of the threats. Of the remaining scenarios, several will be similar enough to group together.

We provide an example to help illustrate the step two process. One concern raised in the policy discussion of stablecoins is the segregation of reserve assets:

> If the reserve assets are not segregated from the equity of the stablecoin issuer, then the investment policy could be misused to privatize returns from the assets whereas losses of the assets would be socialized to the coin holders. (G7 Working Group on Stablecoins 2019, 6)

In this example, the assets are the reserve assets, the threat is the stablecoin issuer, the effect is availability and the method is inappropriate investment of the reserve assets (facilitated by insufficient controls). The risk scenario would also include a time period of assessment and would ask the question in an open-ended manner to signal that we are dealing with uncertainty: "Over the next 12 months, to what extent will the issuer of stablecoin X put the availability of reserve assets at risk through inappropriate investment of the reserve assets?"

We can consider other related scenarios here as well. For example, instead of the stablecoin issuer, a privileged insider such as a portfolio manager could be the threat. Alternatively, the scenario could be silent on the methods used by the issuer to affect the availability of the reserve assets. In such a case, we would consider other methods—for example, outright theft.

Once again, the point of this step is to ensure that all stakeholders in the quantification process understand what is being quantified in order to prevent any misunderstanding. For example, if the legal expert estimates total fines that would occur over 10 years while the security expert estimates the potential frequency over a 12-month period, then the results will suffer.

The process of scoping scenarios also helps identify risk scenarios where preconditions need to be met in order to conduct a loss analysis, so that we can track those preconditions (risk indicators) over time. For example, concerns about the emergence of a global stablecoin (GSC) and its impact on monetary sovereignty (the asset at risk) are unlikely to be realized until:

- a certain level of substitution of the domestic currency for the stablecoin is exceeded
- the stablecoin pays a return that is tied to rates paid on reserve assets
- the proportion of reserve assets in domestic currency is relatively low

These three indicators—substitution away from domestic currency, interest paid to stablecoin users and use of nonreference asset reserves—can be monitored (through the step one process) over time. Once the conditions are met, analysts can then carry out the risk analysis.

Step 3: Quantifying the specific risks

Once concerns have been translated into specific risk scenarios, analysts conducting the assessment[18] can generate quantitative estimates of loss. The expected loss is a function of frequency over a given period (typically a year) times the loss magnitude of the occurrence.

A concrete example will help demonstrate the FAIR analysis process and how authorities can use it to conduct a quantitatively based risk assessment. In the case of a stablecoin arrangement that has yet to launch, authorities could ask a question such as the following:

> If stablecoin X were in use now, over the next 12 months, what is the risk that a cyber criminal group will double spend it (affecting its integrity) via a 51% attack?[19, 20]

To answer this question, the issuer must provide answers to the following:

1. Over the next year, how often will criminal groups double spend stablecoin X via a 51% attack?
2. How much money will stakeholders lose each time a stablecoin X coin is double spent via a 51% attack?

The stablecoin issuer may be able to answer these questions directly, but more likely they will need to break them down further in order to provide a quantitative response.[21] For example, the likelihood of an attack can be broken down into a function of how often criminal groups will attempt it and how likely it is that the stablecoin issuer will be unable to fend off the attack.[22] The losses realized each time criminal groups are successful can be broken down into the losses the stablecoin issuer will incur directly from the attack (its primary losses) and the losses the system of stakeholders will incur indirectly because of the attack on the stablecoin issuer (secondary losses).[23]

The stablecoin issuer will also have to consider the types of primary and secondary losses that could arise, such as:

---

[18] We have been purposely silent on who would conduct the analysis and scenario scoping. It could be the stablecoin issuer, the relevant authority or a third party. For example, relevant authorities could do their own quantitative analysis using this framework and use the resulting exposures as the basis of the discussion with the stablecoin issuer and to iteratively update and improve their assessment of the risk.

[19] A 51% attack refers to an attack on a cryptocurrency where a miner attempts to control more than 50% of a network's mining power. Once the miner has control, they can reverse transactions and double spend coins.

[20] See Orcutt (2019). Although we are specific here in terms of method, authorities could ask this question more generally, requiring the stablecoin issuer to consider the frequency and losses associated with the entire family of transaction verification mechanism attacks used to double spend coins rather than just via 51% attacks.

[21] Appendix B provides a fuller breakdown of this risk scenario.

[22] In the FAIR framework, this is vulnerability or susceptibility to attack. Note that, unlike the way it is normally presented in cyber risk discussions, vulnerability/susceptibility is scenario dependent and almost never zero.

[23] Note that in the FAIR methodology, secondary losses are typically calculated as the losses the firm will incur as a result of actions taken by secondary stakeholders (regulators, clients, media etc.). Here, as authorities, we are interested in the losses incurred by secondary stakeholders, whether or not they are later internalized by the stablecoin arrangement.

- productivity losses from resources becoming idle because the risk scenario has materialized
- response costs from responding to the event (e.g., legal fees)
- replacement costs to replace or repair assets
- competitive advantage costs from the loss of intellectual property or trade secrets
- fines and judgments levied by regulators or the courts, or built into contracts
- reputational damage (e.g., increases in cost of capital, impact on share price, or cost of retaining or attracting staff)

To account for losses in the financial system but not internalized by the stablecoin issuer, authorities may also want issuers to consider such things as the impact on payment flow or assets held in the reserve to back the coin, or the longer-term impacts on the real economy.

Both the authorities and the stablecoin issuer should be able to decompose the risk scenario to the level at which they can draw upon data, expertise or other information to provide calibrated estimates.[24]

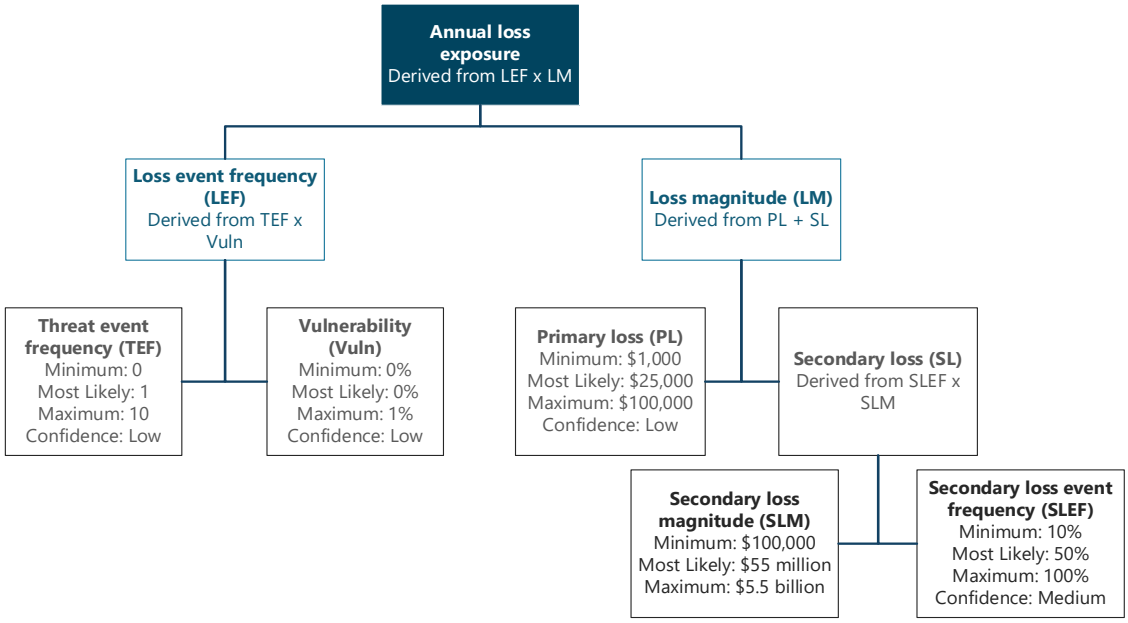
Once the scenario has been sufficiently broken down, the stablecoin issuer, using all available inputs (i.e., data, subject matter experts etc.), should be able to provide a range of values for each part of the risk scenario such that they are highly confident that the true value is contained in the estimate. For example, based on data on attacks on other stablecoins and threat intelligence information, the subject matter expert may be 90 percent confident that the frequency of 51% attacks over the next 12 months is a minimum of zero and a maximum of 10 times. They may determine it is most likely that one such attack will take place, but based on the quality of the data and their level of certainty about the most likely number of attacks, the probability between the lowest and highest frequency can be assumed to be uniformly spread.[25]

In a similar way, the stablecoin issuer, using available data, subject matter expertise from legal and cyber response experts, can provide ranges for response costs, legal judgments and other values on the loss magnitude side. Examples of resulting values and ranges are provided in **Figure 7**.

[24] For example, if there is no information or reliable estimates of how often criminal groups will attempt a 51% attack, then the problem can be broken down further into a function of the number of times criminal groups will come into contact with the assets necessary to conduct the attack and the probability that when they come into contact with the assets, they will take action.

[25] In the FAIR framework, a modified PERT distribution is used for the simulation; however, other distributions may be used depending on the data available. The PERT distribution requires four parameters: the minimum, the maximum, the most likely values of the estimate and a parameter to control how much weight is allotted to the tails. A low confidence in the most likely value results in a fairly uniform distribution. PERT stands for program evaluation and review technique. The distribution used in that technique is the PERT distribution. Here, an additional parameter is added to the PERT distribution to allow it to take on a wider range of non-normal distributions.

Figure 7: Model ontology and input values



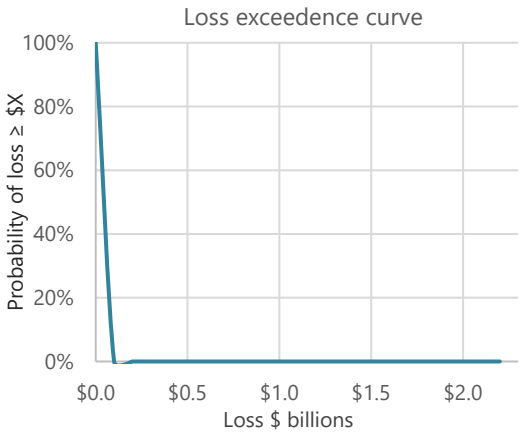
Once the ranges are determined, the stablecoin issuer can simulate the scenario by random draws from distributions calibrated by the expert parameters. An example of the output of this process using the example values provided above is shown in **Figure 8**.

Figure 8: Monte Carlo simulation results—51% attack

Frequency and loss

	Min	Avg	Max
Primary losses			
Loss event/year	0	0.01	1
Loss magnitude	$1.2K	$33.2K	$93.1K
Secondary			
Loss event/year	0	0	1
Loss magnitude	$3.4M	$946.2M	$4.7B
Vulnerability/Susceptibility		0.28%	

Annualized loss exposure: $0 (Min), $4M (Avg), $2.2B (Max)



The simulation output provides estimates for both frequency and loss, including separate estimates for primary and secondary losses. In this stylized example, the resulting frequency is rare, occurring on average once every 100 years, with secondary losses occurring even more infrequently. The simulation result suggests that in rare cases significant secondary losses can

occur. The double spending of stablecoin and devaluation of all existing stablecoins could result in a loss of $2.2 billion and, further in the tail, a loss of $4.7 billion.

Whether relevant authorities are concerned about these results will depend on their assessment of the loss capacity of the stablecoin arrangement, affected stakeholders and the financial system generally. Authorities will also be guided by the loss tolerances allowed in applicable domestic and international rules and regulations. If the results exceed these thresholds, the risk analysis can then be used to identify potential controls and quantitatively evaluate loss reductions.[26]

Conclusion

We have outlined a three-step method to investigate stablecoin arrangements and quantitatively assess their risk. Following this approach has advantages: it allows relevant authorities and stablecoin issuers to be specific about their concerns and to be more consistent in their treatment of stablecoin arrangements.

Relevant authorities can audit the issuer's risk assessments, asking what data, subject matter expertise or other information was used to determine, for example, threat frequency, contact frequency, or secondary loss fines and judgments. They can also ask whether the basis for these estimates are adequate or whether the issuer should be seeking better information.

Compared with existing qualitative approaches to measuring risk, the three-step method allows for more frequent and more rapid revision of estimated loss and frequency as conditions change or as new data become available. Stablecoin issuers can easily consider potential controls and demonstrate their effectiveness to authorities.

Finally, the most important benefit of the three-step method is that it allows for a shared understanding between authorities and the stablecoin arrangement about the size and nature of potential loss exposures. To have a meaningful dialogue with issuers and to set effective standards that do not stifle innovation, relevant authorities need in-depth knowledge of the stablecoin arrangements coming to the market, a clear understanding of their own concerns and a quantitative basis for discussion. The three-step approach outlined here can help them achieve this.

[26] Controls here are only those measures that can be shown to reduce losses by reducing either loss event frequency or loss magnitude.

References

Bailey, A. 2020. "Reinventing the Wheel (With More Automation)." Speech at the Brookings Institution (virtual event) September 3.

Chambers, C. 2019. "Bitcoin Really Is Money, Here's Why." *Forbes*, February 15.

Financial Crimes Enforcement Network. 2013. *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*. Washington: US Department of the Treasury.

Financial Stability Board. 2020. *Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements*. Basel: The Financial Stability Board.

Freund, J. and J. Jones. 2015. *Measuring and Managing Information Risk: A FAIR Approach*. Oxford: Elsevier.

G7 Working Group on Stablecoins. 2019. "Investigating the Impact of Global Stablecoins." Committee on Payments and Market Infrastructures Paper No. 187.

Hubert, F. 2016. "Opinion." *BaFin 2016 Annual Report*. Bonn: Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin).

Lautenschläger, S. 2019. "A Supervisory Perspective on 2019 and Beyond." Speech at the Risk Management and Supervisory Conference, Banking and Payments Federation Ireland, Dublin, Ireland, January 17.

McBride, S. 2020. "You Can Now Buy Bitcoin on PayPal For $1." *Forbes*, December 4.

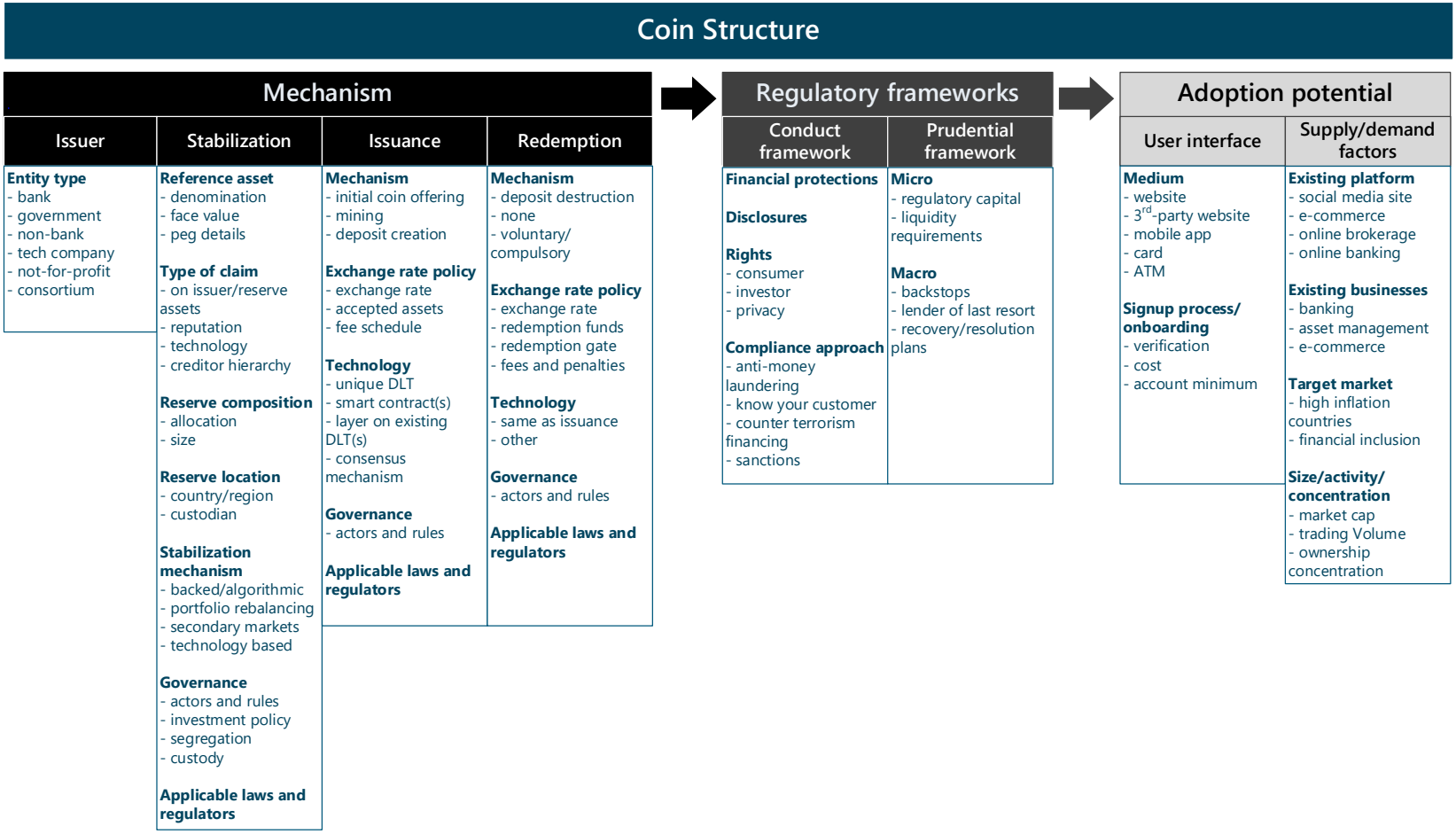
Orcutt M. 2019. "Once Hailed as Unhackable, Blockchains Are Now Getting Hacked." *MIT Technology Review*, February 19.

President's Working Group on Financial Markets. 2020. "Statement on Key Regulatory and Supervisory Issues Relevant to Certain Stablecoins." US Department of the Treasury, December 23.

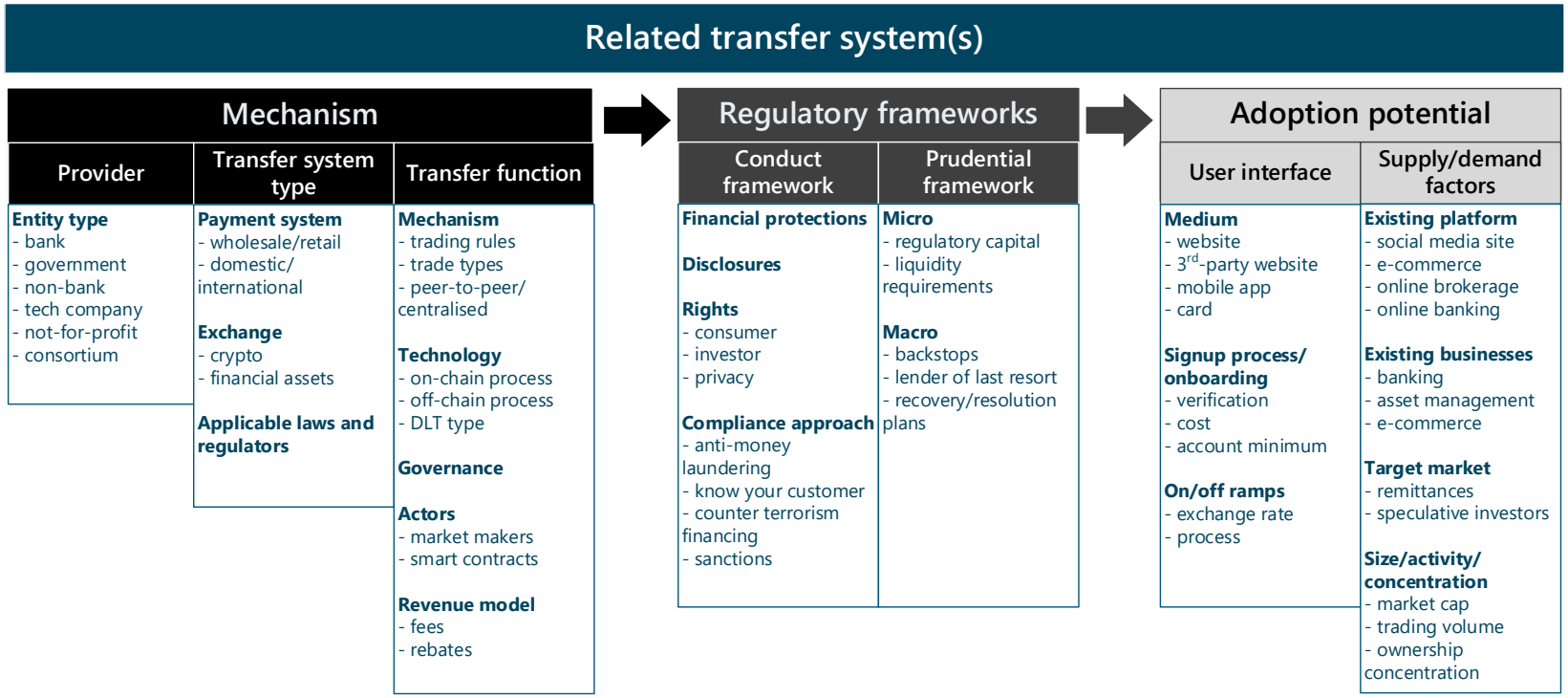
Restoy, F. 2019. "Regulating Fintech: What Is Going On, and Where Are the Challenges?" Speech at the ASBA-BID-FELABAN XVI Banking Public-Private Sector Regional Policy Dialogue, "Challenges and Opportunities in the New Financial Ecosystem," Washington DC, October 17.

Appendices

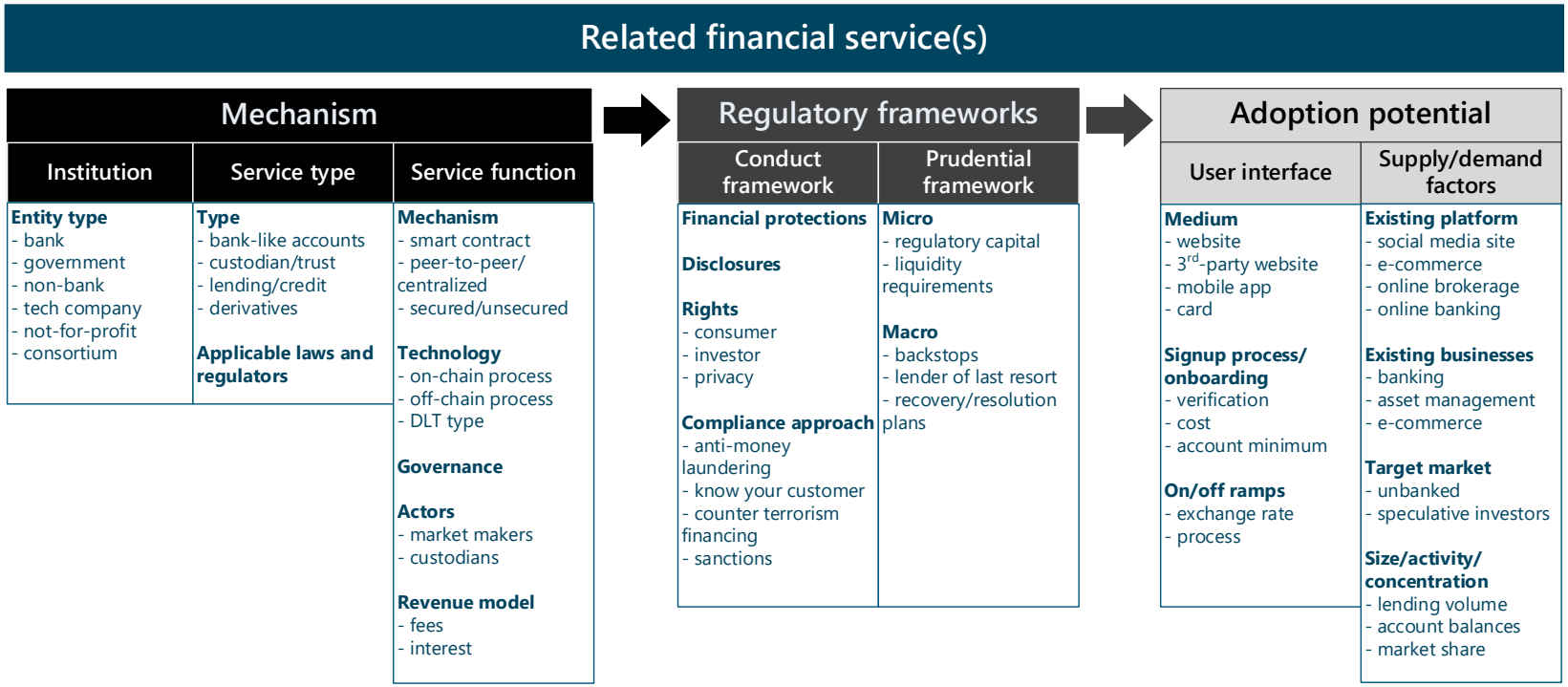
Appendix A: Complete categorization of the coin structure



Appendix B: Complete categorization of the related transfer system(s)



Appendix C: Complete categorization of the related financial service(s)



Appendix D: Example scoping table

			Threats																														
			Criminals			Nation states			Terrorists			Stablecoin users (retail/wholesale)			Stablecoin issuer			Stablecoin issuer insiders			DLT participants			Market makers/Other intermediaries			Other investors			3rd-party suppliers		
Effect (C-Confidentiality, I-Integrity, A-Availability)			C	I	A	C	I	A	C	I	A	C	I	A	C	I	A	C	I	A	C	I	A	C	I	A	C	I	A	C	I	A
Assets	Monetary	Reserve currency(ies)																															
		Short-term securities																															
		Other reserve assets																															
	Data	Personally identifiable information (PII)																															
		Business operations data																															
		System data																															
		Transaction logs																															
	Sovereignty	Tax revenues																															
		Price stability																															
		Financial stability																															
		Limitation of illicit activity																															
		Gross domestic product																															

Appendix E: Example decomposition of a risk scenario