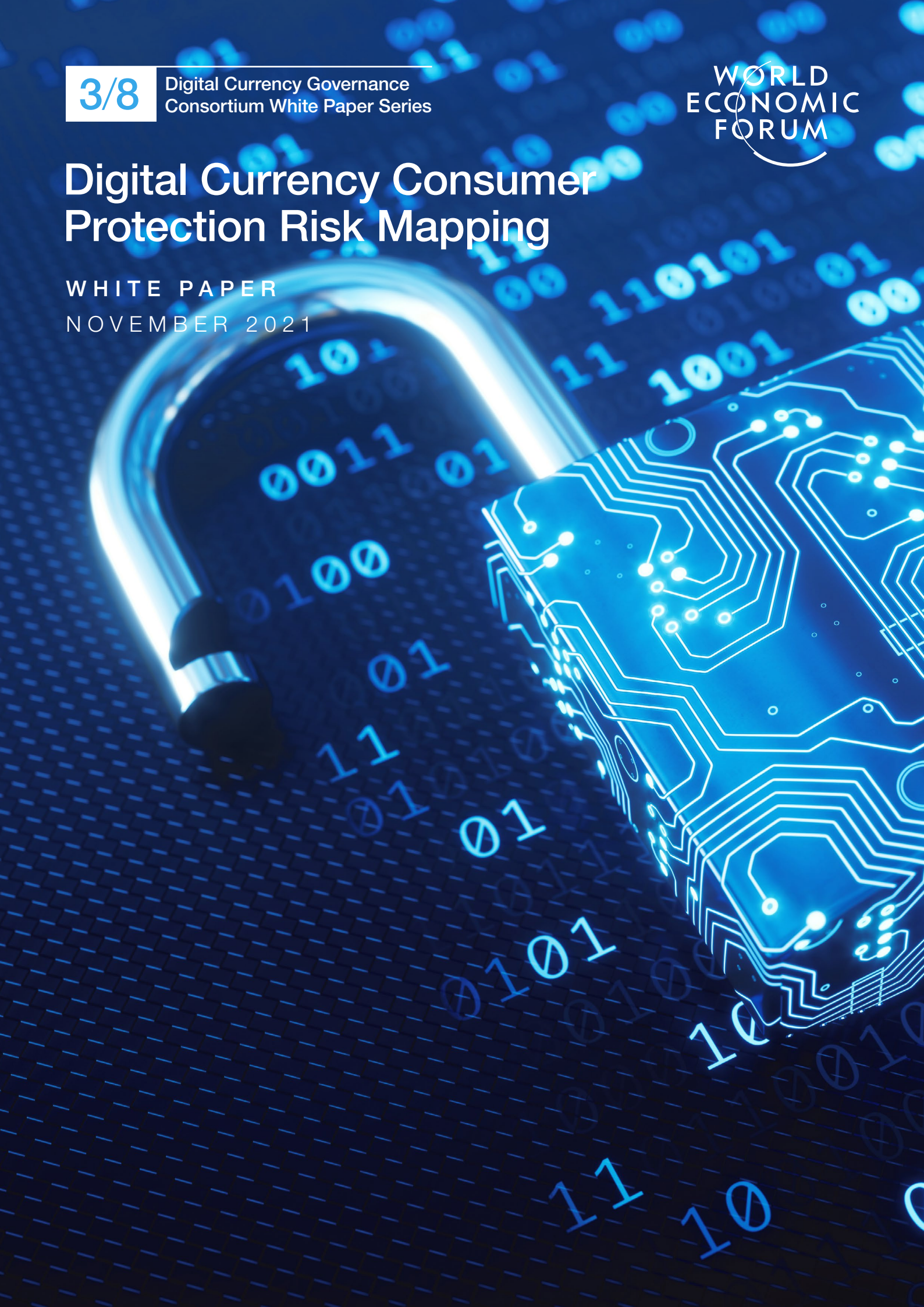
3/8 Digital Currency Governance Consortium White Paper Series

WORLD ECONOMIC FORUM

Digital Currency Consumer Protection Risk Mapping

WHITE PAPER

NOVEMBER 2021



Images: Getty Images

Contents

This white paper is part of the Digital Currency Governance Consortium White Paper Series. Its authors, contributors and acknowledgements can be found in that compendium report.

Preface

This white paper maps the risks of using various forms of digital currency, compared with existing forms of payment and currency. These insights could inform the drafting of principles for consumer protection for each type of digital currency.

With each advancement in payment technology, consumers face new opportunities, but also new challenges and risks, not all of which are easily perceptible. This was certainly the case with the introduction of e-money, which presented new concerns around information disclosure and variability in regulatory regimes, to name a few.[1] In the context of stablecoins, some of these challenges are already becoming clear, such as ambiguity in redemption rights and schemes backing the valuation. Assuming that consumer trust is critical for adoption, careful consideration of appropriate consumer protections is warranted before central bank digital currencies (CBDCs) or stablecoins are moved into widespread use.[2]

It is important to note that one of the reasons innovation occurs is in response to consumer demand; that is, new approaches are often (though not exclusively) developed to meet a need or provide a new benefit. It is essential to preserve these benefits while also ensuring protection and safety. This balance can be achieved by examining the totality of options available to consumers and assessing the relative risks and benefits that exist within the relevant context. Furthermore, it is important to note the potential for regulation to stifle both competition and innovation if it is not inclusively developed.

This paper sets out a typology of risks to consumers, associated with different digital currencies and different technology and governance options. Our analysis aims to help consumers, consumer-rights advocacy groups and policy-makers to better understand the risks. It also provides some high-level principles to guide policy-makers and regulators in designing an effective and coordinated consumer protection programme, as well as in identifying who owes duties to consumers in this context.

1 The risk landscape of digital currencies

This chapter addresses three broad areas of the risk landscape associated with the introduction of digital currencies:

- Key issues to consider when mapping risks posed by digital currencies
- The notion of consumer protection in digital currency
- The general risk to consumers where newer products mimic legacy products and appear familiar, without the technology underpinning them being subject to a similar regulatory framework

1.1 Key issues to consider when mapping risks posed by digital currencies

As discussed in more detail below, some of the key issues to consider when mapping the risks posed by digital currencies include the following:

- Stablecoins and CBDCs may carry different risks and benefits to consumers
- Risks may differ according to context, including across different types of users
- Not all risks are equal; some top-line consumer risks may warrant special attention
- Different ways of using digital currencies can attract different types of risk
- Accountability can be difficult to determine and enforce in stablecoin ecosystems

Our approach to mapping the risks posed by digital currencies is demonstrated in the graphic at Figure 1.

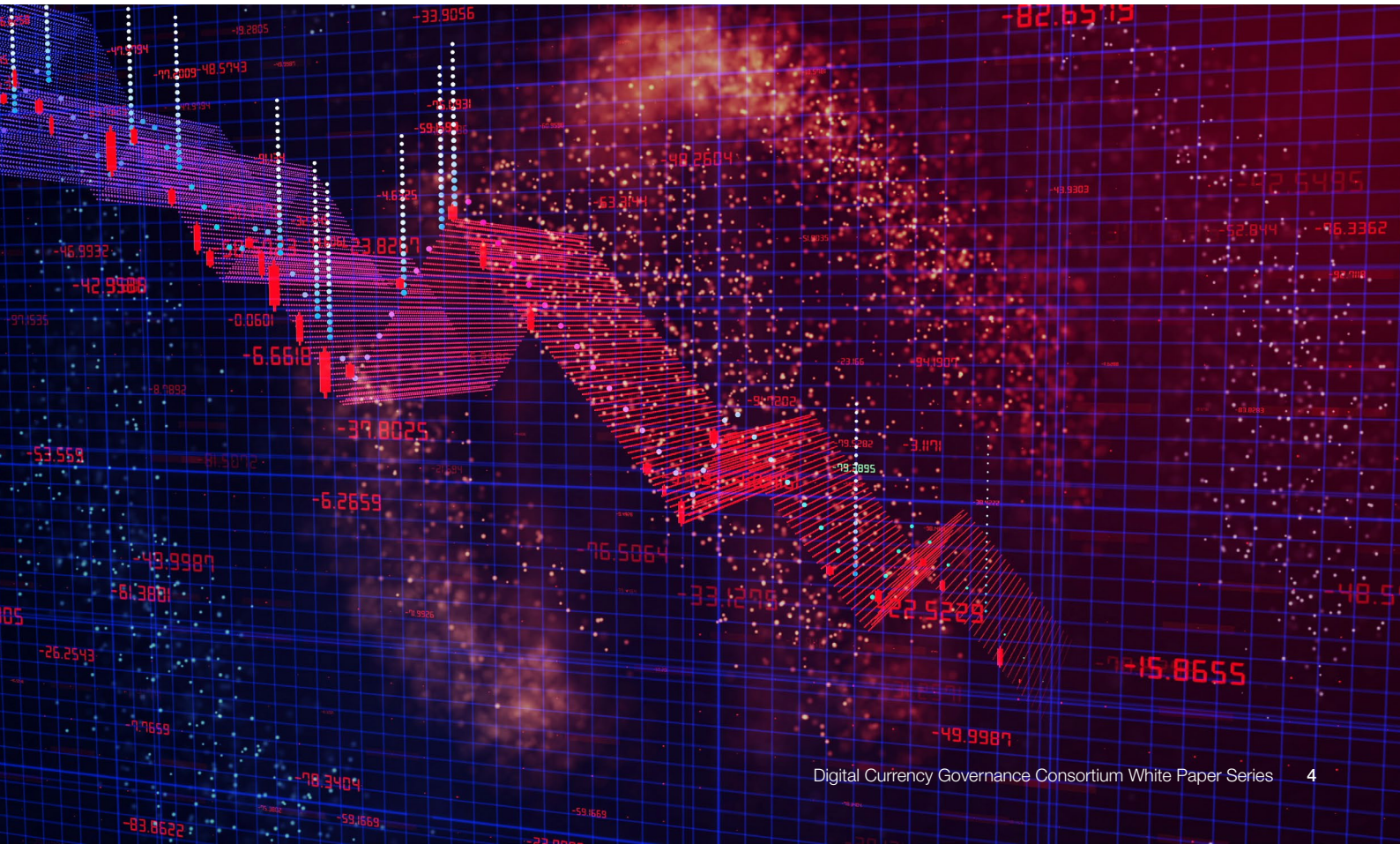
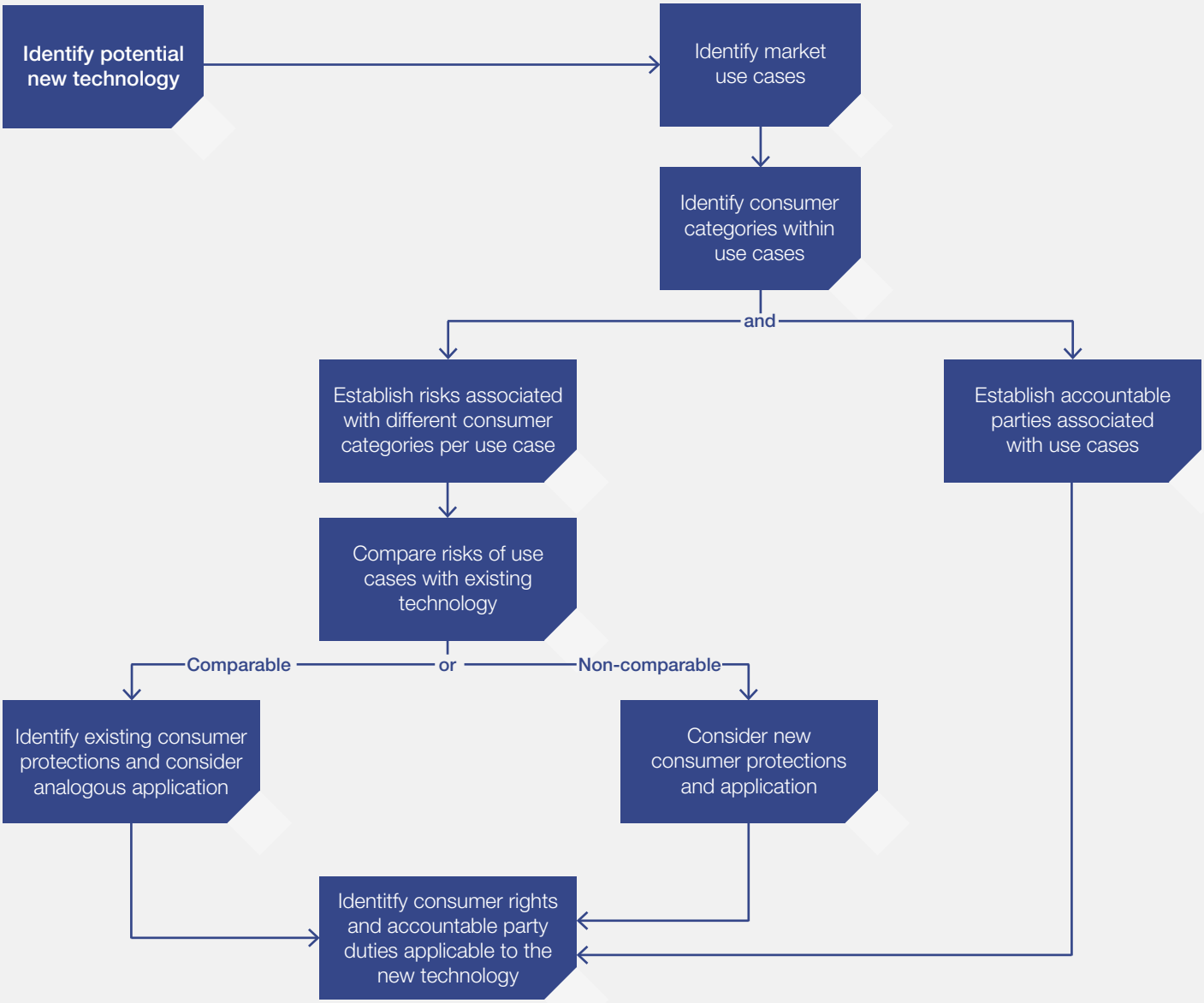


FIGURE 1 | **A suggested approach to mapping the risks posed by digital currencies**



Stablecoins and CBDCs may carry different risks and benefits to consumers

Generally, the risks that consumers face when using stablecoins may be of a different class from those posed by CBDCs. Whereas a CBDC carries the weight of the issuing central bank, a primary concern with stablecoins, in the context of consumer protection, is value and backing. Stabilization methodologies used to maintain the value of stablecoins are affected by a variety of concerns, such as the credibility and willingness of the issuer to maintain the stabilization and reserve backing, the choice of backing mechanism, the types of governance structures, the way the issuance is managed and the redemption and technical choices that are made.[3]

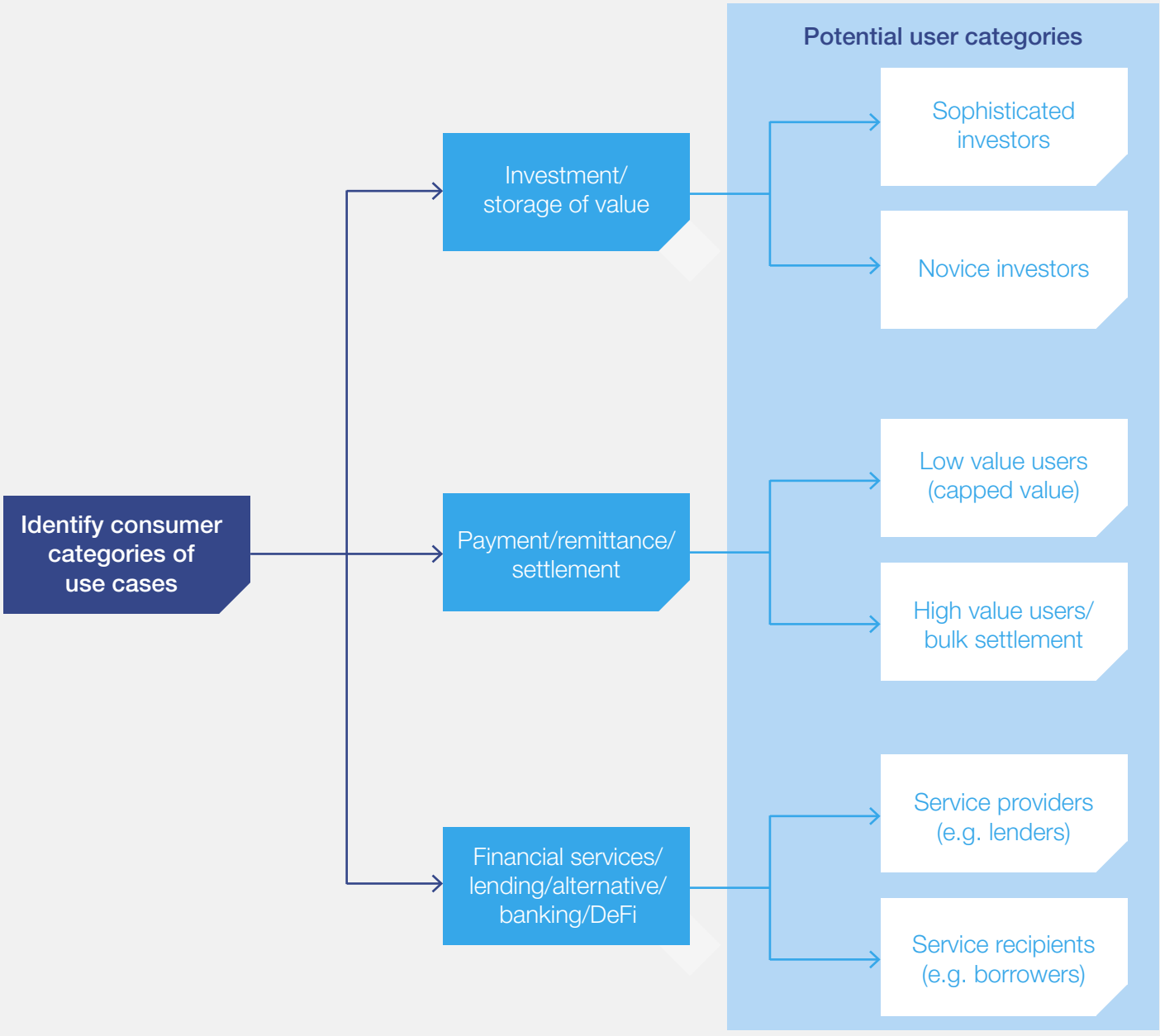
As a CBDC constitutes a direct central bank liability, CBDCs benefit from tested architecture to preserve value. On the other hand, CBDCs may present privacy issues, depending on their design.[4] For a more detailed discussion on potential privacy design choices for CBDCs, please refer to the white paper in this series entitled *Privacy and Confidentiality Options for Central Bank Digital Currency*.

This white paper focuses primarily on *stablecoin* consumer protection issues, while also mentioning where these may be relevant to CBDCs.

Risks may vary according to different types of users

In identifying risks, this paper acknowledges that risks may differ across different types of users. This is particularly true in the case of stablecoins, where some of the applications result in different potential users. In this paper, the term "users" refers to everyone who participates in distributing and holding digital currencies, while the term "consumers" refers to the end-users, whose interests would typically be subject to consumer protection policy and regulation in the face of new technology. Figure 2 shows examples of potential user categories, which may affect choices made in respect of consumer risk mitigation. The figure is not intended to be an exhaustive list, but rather a high-level example of use-case categorization.

FIGURE 2 **An example of potential user categories**



Some top-line consumer risks warrant special attention

In carrying out a mapping of consumer risk areas, an exhaustive approach creates the potential for blind spots and over-comparison, particularly in a new and fast-developing sector. Nonetheless, Figure 3 highlights some top-line consumer risks that warrant special attention, due to their widespread nature and the danger they pose to both the individual consumer and the wider public.

FIGURE 3 | **Top-line consumer risks**

Different ways of using stablecoins can attract different types of risk

Users may employ stablecoins for different purposes and have different levels of involvement in the governance of stablecoin protocols. Stablecoins were arguably invented to enable investors to trade cryptocurrencies and to hold blockchain-enabled assets without suffering from the volatility of cryptocurrency prices in their investments and other activities. Based on a report published by the Block Research in March 2021, the average transaction size for stablecoins was $9,000 in 2020.[5] The high average transaction value suggests that most users of stablecoins are engaged more with investment than retail buying or selling. Depending on their usage and roles, stablecoin users may be exposed to different types of risks.[6]

Figure 4 lays out different uses of stablecoins across different categories of users, along with the associated risks.

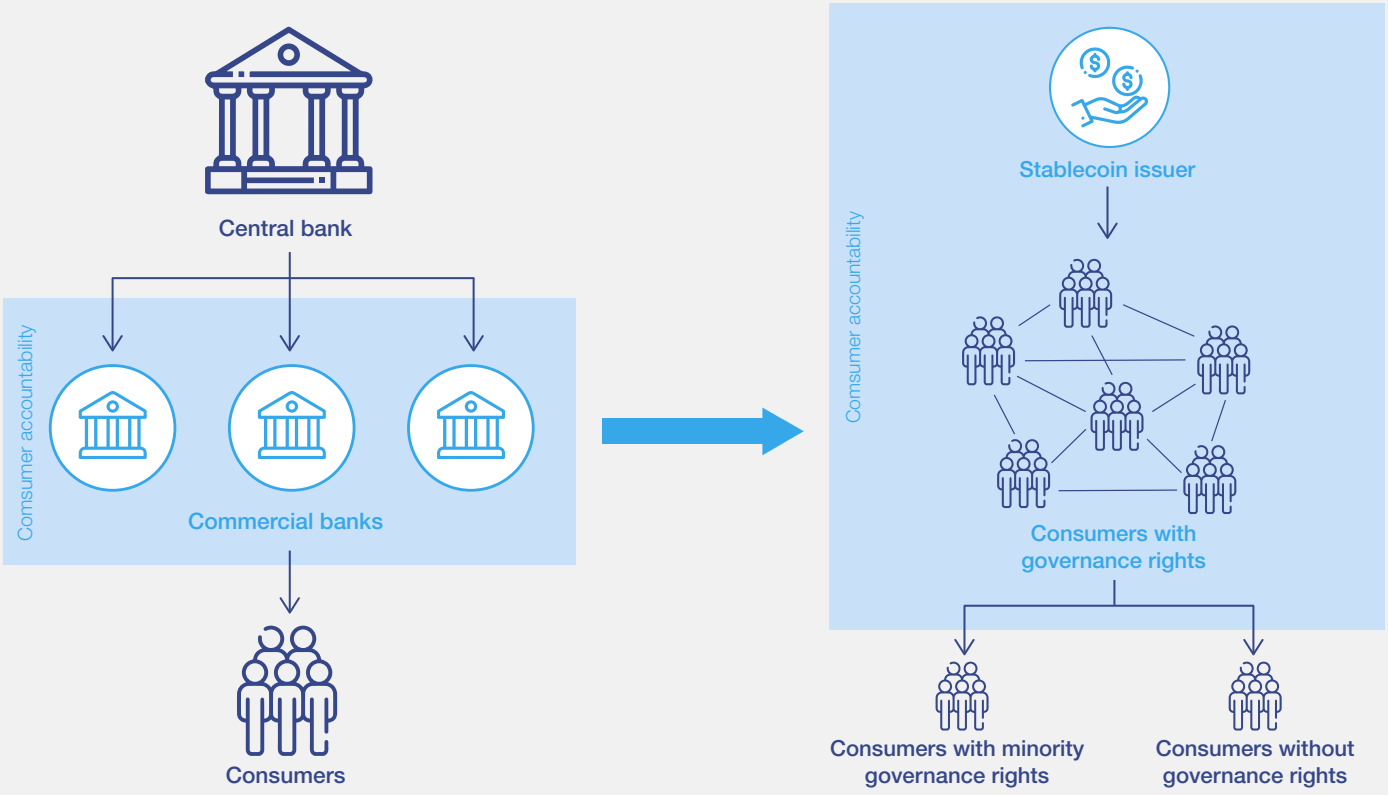
FIGURE 4 | **Risks associated with different uses of stablecoins**

	Investor	Retail buyer/seller	Participant of protocol governance[7]
Stablecoin usage	– Provide capital denominated in stablecoin to earn a return – Park money for future trading of cryptocurrencies	– Exchange for goods/services	– Can be either an investor or a retail buyer/seller
Risk	– Inability to redeem face value – Deposit liability claim – Price volatility	– Inability to redeem face value – Deposit liability claim – Price volatility	– Rights being infringed by majority holders

In stablecoin ecosystems, who should be accountable to consumers?

Owing to more decentralized management, accountability can be difficult to determine and enforce in the case of stablecoins[8]. With traditional central bank systems such as cash, commercial banks – as the distributors of money – provide consumer protections and guarantees,[9] and accountability tends to be easily determinable in bilateral engagements with consumers (see the left half of Figure 5). Policy-makers are now facing a new question: In stablecoin ecosystems, who should be accountable to consumers? (see the right half of Figure 5).

FIGURE 5 | **Who protects consumers in stablecoin ecosystems?**



1.2 Challenges around consumer protection in digital currency

Consumer protection and the challenges that arise when blockchain-based digital currencies are used for the purposes of payment have been addressed by regulators in a variety of ways. Often, initial consumer protection takes the form of restrictions or, in some instances, bans on the use of such digital assets. Several regulators have given warnings to consumers of their risks, as was seen in the growth of Bitcoin, for example.[10] Some jurisdictions, such as China, have gone as far as banning cryptocurrency trading altogether.[11]

In recent years, there have been attempts to draw cryptoassets into existing regulatory frameworks. In June 2019, for example, the Financial Action Task Force (FATF) revised its standards in respect of virtual asset service providers (VASPs), to apply anti-money laundering/combating the financing of terrorism (AML/CFT) requirements to virtual assets and their service providers (this was under review in 2021). The decentralized nature of cryptocurrencies and stablecoins, and how they are used, has often presented the biggest regulatory hurdle, as regulators struggle to determine which among them is responsible for regulation and how to enforce such regulation. These struggles have frustrated the creation of regulatory frameworks. As it is difficult to identify an individual or central organization which consumers can hold to account, protection and regulation have typically targeted the exchange of such assets in and out of fiat, for example crypto-exchanges and banks.

However, the evolution of digital assets and the emergence of privately issued stablecoins have moved the discussion beyond individual consumer risks. There has recently been a greater focus on the potential wider impacts to financial markets and to the public at large, with some pointing to dangers posed by the risk of large price movements or "runs", with rapid selling and withdrawals, particularly where stablecoins may not be fully backed by reserves[12]. The largest stablecoin, Tether – most often used as a medium of exchange in cryptocurrency trading – ties its value to the US dollar and has $62 billion of outstanding tokens at the time of writing. However, it does not fully back its tokens with US dollar reserves and has, at times, held significant shortfalls; it has also been found to repeatedly mislead clients about its reserves.[13]

Beyond the regulation of "on- and off-ramps" at national and supranational levels, proposed legislation is now emerging that seeks to regulate the use of digital assets in financial services.[14] Of course, this begs the question of how the assets are used and which regulator should do the regulating.

> When stablecoins are not fully backed by reserves, it may lead to significant dangers posed by the risk of large price movements or runs

1.3 The general risk to consumers of familiarity without a regulatory framework

Most ordinary consumers do not understand the difference between public money (fiat currencies issued and backed by central banks) and private money (money held in commercial bank deposits, which is a liability of private entities). In particular, the average consumer is often unaware that notes and coins issued by a central bank carry a claim against the central bank, which is passed on once those notes and coins are deposited into a bank account – that is to say, they become private money guaranteed to the extent of the local deposit guarantee scheme.

It is likely that firms in the blockchain industry will provide products and services that are similar in nature to those used by consumers today. This similarity, however, can be misleading as consumers may not understand the different protections (or lack thereof) that apply to different payment services – particularly given the rudimentary understanding of current systems by the average consumer – and may therefore not undertake fully informed risk assessments. For example, a purchase of groceries from a banking application, e-money wallet or stablecoin wallet may require consumers to undertake similar onboarding processes and payment flows. There are likely to be similar security requirements that consumers undertake to access their wallets. However, a payment that is inadvertently sent to the wrong merchant may result in different consequences depending on the payment type and local law.

This creates a risk of familiarity without protection, where equivalent regulatory frameworks have not yet been put in place for digital currency. When consumers perceive payment forms to be similar, they are more likely to behave in the same way as they would with legacy products or services, rather than watching out for new risks or taking care around similar risks in the digital space which lack the regulatory protection provided to legacy products.

2 Specific top-line consumer risks

This chapter addresses the following six top-line consumer risks, identified in Figure 3:

1. Risks associated with value and backing
2. Risks associated with inadequate depositor protection
3. Payment risks
4. Privacy risks
5. Security & technology risks
6. Accountability risks

These risks do not present the same degree of danger across all forms of currency. Before analysing these risks in the context of stablecoins and CBDCs, it is worth considering these same risks within existing systems (see Figure 6). It is important to note that stablecoins and CBDCs are far from monolithic, and design choices can significantly affect both the presence and magnitude of risks. In addition, the areas in red below are areas garnering significant attention from regulators and policy-makers, which could lead to changes that decrease the level of consumer risk.

FIGURE 6 **Comparison of current top-line consumer risks in existing systems and in digital currencies**

	Value & backing risks	Depositor protection risks	Payment risks	Privacy risks	Security & technology risks	Accountability risks
Cash	Backed by central bank	N/A	Fraud and theft	High level of privacy from all parties except direct recipient (payee)	At risk of counterfeiting	Depends on issue; payee responsible for accepting legitimate cash
E-money	Reliant on depositor protection	Two-layer risks (wallet-provider and deposit-taking institution where wallet-providers deposit customer funds)	Typically protected from user error and by debit guarantees	Account-based: dependent on privacy laws of country	Relatively secure and tested	Bank and wallet-providers accountable
Commercial bank money	Same as e-money	High degree of standardized protections and regulation	Same as e-money	Same as e-money	Same as e-money	Bank accountable
Stablecoins	Variety of backing mechanisms which carry different risks[15]	Varied: typically no or limited depositor protections	Limited examples of protections equivalent to bank money or e-money	Varied: governance systems differ on privacy. Many institutions push privacy obligations to VASPs	Varied: audit standards still to be fully developed Varied: Counter-feiting risk in the form of double spend	Unclear - See Fig. 5
CBDC	Same as cash	N/A	Some risk depending on architecture (e.g. in "push" vs "pull" transactions)	Dependent on design & architecture (see Privacy white paper)	Dependent on design & architecture. Early pilots reveal focus on security standards and the prevention of hacking or breach[16] Varied: Counter-feiting risk in the form of double spend or illegitimate copying of CBDC	Central bank accountable

High consumer risk · Medium consumer risk · Low consumer risk

2.1 Risks associated with value and backing

As discussed previously, stablecoins vary widely in their design, making it challenging to generalize about their risk profile. Detailed analysis of each offering is necessary to evaluate risk. Nevertheless, at present the lack of clear regulatory or other guidance means that it is likely that there will be ongoing challenges in maintaining the price stability of the reference assets of stablecoins. The term "stablecoin" itself can be misleading, as stablecoins may lose their ability to hold steady value relative to their reference asset (see Figure 7) and consumers are not universally guaranteed that stablecoins are free of underlying volatility.

Policy-makers will need to consider whether deposit insurance is appropriate in the same way as required for regulated financial institutions

With traditional currencies, consumers expect to be able to redeem the value of their deposits on a 1:1 basis, at any time. However, where proceeds from a stablecoin sale are held not in a depository account but in financial assets, such as securities or government bonds, with varying levels of risk exposure (which may not fully back outstanding stablecoins), the value of the stablecoin is also subject to such risk exposure. In addition, a lack of regulatory guidelines on the relevant governance and risk management policies of the issuer and its reserve management creates further risk exposure, which is not present with traditional bank deposits. This is further exacerbated by a lack of standardization of terms such as "stable", "backed by" or "backing" used in the marketing of many privately issued stablecoins. These terms often oversimplify the complex and varied forms of stablecoin collateralization, which include the following:

- **100% backed by funds**:[17] where stablecoins are backed by reserve funds that the stablecoin-issuer or custodian holds for safekeeping, implying a commitment to their full redeemability in fiat currency.
- **Off-chain collateralization**: where stablecoins are backed by assets held off the distributed ledger, often with a custodian for safekeeping.
- **On-chain collateralization/crypto-backed**: where stablecoins are backed by assets on the distributed ledger, which are capable of being recorded in a decentralized manner on the blockchain and may not require a custodian.
- **Algorithmic collateralization**: where stablecoins are backed using some form of price stabilization algorithm to track a particular unit price (usually linked to the US dollar) and where such backing is reliant on the expectations of users on the future purchasing power of their holdings. This form of backing does not need the custody of any underlying asset; it operates fully on-chain and in a decentralized manner.

These different forms of backing carry with them different consumer risks.[18] Figure 7 sets out these different types of stablecoin collateralization and their associated risks to the consumer.

FIGURE 7 **Different ways of backing stablecoins and their potential risks**

	100% backed by funds	Off-chain collateralization	On-chain collateralization	Algorithmic collateralization
Is there an accountable party if there is an issue with the backing mechanism?	Yes	Yes	No (replaced with smart contract)	No (replaced with smart contract)
Potential consumer risks	Fraud and operational risk (e.g. insufficient funds to quickly meet redemptions) High risk and susceptible to confidence crises or a run on the stablecoin if the funds are not legitimate or sufficiently liquid	Linked to underlying collateral and dependent on whether that value is fixed or fluctuates	High risk as collateral is volatile by nature	High risk and susceptible to confidence crises or a run on the stablecoin

For each type of stablecoin backing, it is important to be clear on whether and to what extent the consumer bears the risks associated with that collateralization. Where a redemption based on a fixed ratio is guaranteed, the issuer will typically bear liability for fluctuations from the fixed redemption price resulting from its reserve assets' risk exposure. Such an approach is more akin to traditional bank deposits and can inspire greater consumer confidence (even though most commercial bank deposits have deposit insurance protecting against risks such as theft or bank bankruptcy).

However, where the consumer bears the risk, the value of the stablecoin in the consumer's hands will fluctuate in line with the underlying reserve asset. Such exposure could dissuade widespread adoption, influence consumer confidence and result in mass withdrawals, destabilizing the value of the stablecoin further. This is amplified by the fact that, in such mass withdrawal events, consumers are unlikely to be protected by the traditional depositor scheme protections available for bank deposits or benefit from central bank protection as the lender of last resort. Other circumstances which could trigger mass withdrawals include the circumstances of the issuer, such as a change in governance or critical rules, or technological risks such as cyberattacks.

It is crucial for issuers to be transparent about forms of backing and their associated risks, and for consumers to be properly educated on the underlying value protections (or lack thereof) when compared to traditional bank deposits or e-money. Consumers will also need to be informed of new risks, such as those mentioned above, and how these may trigger a crisis of confidence among users that threatens the "at par" redeemability of stablecoins. Lastly, issuers should inform consumers of whether the redemption value is fixed at par and who bears the risk with respect to the volatility of the underlying assets. The practical feasibility of such education and transparency measures also needs to be assessed from jurisdiction to jurisdiction, as for some it may be more expedient and cost-effective to consider some form of "qualified investor" threshold instead.

2.2 Risks associated with inadequate depositor protection

> In the case of bankruptcy of the depository institution, e-money consumers may only get back a portion of their money unless the e-wallet or mobile wallet-providers are sufficiently capitalized

Deposit insurance is designed to protect consumers from the risk of bankruptcy of deposit-taking financial institutions. When it comes to e-money, there are two layers of consumer risks with respect to the money held by e-wallet service providers, which may also apply to digital currencies if they are held in a custodial account:[19]

- Risk of bankruptcy of the e-wallet service provider
- Risk of bankruptcy of the deposit-taking institution where the e-wallet service provider deposits its customers' funds

To address the first risk, countries often require e-wallet service providers to be sufficiently funded and to set aside a certain percentage of their fund liabilities in a custodian account with a deposit-taking financial institution. Since e-money providers do not typically leverage their balances, policy-makers will need to consider whether deposit insurance is appropriate in the same way as required for regulated financial institutions. A limited number of jurisdictions require e-wallet-providers to obtain a banking licence and subject all consumer accounts to deposit insurance, hence protecting e-wallet-providers from bankruptcy. China goes a step further by requiring e-wallet or mobile wallet-providers to deposit 100% of their customers' funds either with a commercial bank or with the central bank. In the European Union (EU), if e-wallet or mobile wallet providers purchase private insurance to cover any unfunded liabilities, they would not need to deposit customers' funds with an insured depository institution.[20]

In jurisdictions where banking licences are not required for e-money services, balances in e-wallets or mobile wallets are not considered as deposits and e-wallet-providers are usually not required to obtain deposit insurance to cover individual accounts they hold.[21] While e-wallet or mobile wallet-providers may deposit their customers' funds with an insured depository institution, the custodian account is protected up to the coverage limit of the deposit insurance. In the case of bankruptcy of the depository institution, e-money consumers may only get back a portion of their money unless the e-wallet or mobile wallet-providers are sufficiently capitalized.

Limited jurisdictions, such as the US, offer a "pass-through" approach, which allows each individual e-money account to be covered by the coverage limit of the deposit insurance.[22] The "pass-through" approach offers more protection to individual e-money consumers against the bankruptcy of depository institutions. In the case of emerging economies such as Kenya, the electronic value must be backed by a corresponding value in bank accounts. These bank accounts are essentially trust accounts that should ideally be independent and ring-fenced from any possible bankruptcy of the e-wallet provider. The challenge with this approach is that, for deposit protection purposes, the bank trust account is treated as one account and may not compensate the various underlying wallet holders. To mitigate this risk, regulators set stringent conditions for these funds to be held in various reputable and financially sound banks and invested in liquid assets, particularly government securities.

2.3 Payment risks

Different payment methods carry different consumer protections. For example, cash is 100% guaranteed by a central bank, and typically carries the status of legal tender. However, cash provides no inherent user protection in the case of loss or theft.

When placed into an account with a commercial bank, cash transforms into commercial bank money and is guaranteed, in the event of bank insolvency, to the extent of (for example) the applicable deposit guarantee schemes. Payments made using commercial bank money in many jurisdictions carry with them varying degrees of regulatory consumer protection for bank error, user error and debit guarantees, such as the Direct Debit Guarantee in the UK (a consumer reassurance system which provides protection for payment errors).[23] Although these protections are still to some degree reliant upon consumers identifying an error and making a claim, protections such as deposit insurance and the oversight of monitoring and regulatory authorities remain available.

When cash and commercial bank money is used to purchase electronic money, it becomes electronic money or "e-money". Within the EU and UK, for example, electronic money has the same regulatory protections as payments made with commercial bank money and benefits from the right of at-par redeemability.

Stablecoins that are not considered e-money at present carry no similar regulatory consumer protections for payments. For instance, under the proposed EU regulation on Markets in Crypto-assets (MiCA),[24] fewer consumer protections are available for payments made with tokens that are stabilized using assets (asset-referenced tokens or stablecoins) than for payments made with e-money tokens,[25] since asset-referenced stablecoins do not fall within the definition of funds under Payment Services Directive 2 (PSD2 – the European directive for electronic payment services).[26] This gap in protections for payments using stablecoins was identified an issue to be addressed in the recent UK consultation for a regulatory framework for cryptoassets and stablecoins.[27]

Even though both CBDCs and stablecoins are generally intended by their creators to serve as a payment medium similar to cash, bank money and e-money, some functionalities of CBDCs and stablecoins may differ from existing options and are worth highlighting to consumers. The "push" versus "pull" distinction in terms of payment mechanism is a good example. A push transaction refers to a transaction where it is initiated by the payer, who needs to know the name of the payee's financial institution and their account number. A pull transaction refers to a transaction where it is initiated by the payee and the payee needs to know the name of the payer's financial institution and their account information.

While both types of transactions are subject to cybersecurity risks,[28] a push transaction is fundamentally less risky than a pull transaction for both the payer and the payee, since only the account with sufficient funds could make the transaction happen. In contrast, a pull transaction could bounce because the payee has no visibility of the balance the payer has in his or her account. Currently, it is debatable whether transactions made in stablecoins will be push-only transactions, given the technology may enable automatic payment upon fulfilment of certain conditions. By contrast, transactions made through cards and bank accounts can be either push or pull transactions. Depending on their technical choice and how accounts are structured, CBDCs may facilitate either push or pull transactions.

2.4 Privacy risks

Given that stablecoins are typically privately operated, they are susceptible to business practices and models prevalent in the technology industry. For example, this may include business practices developed in unregulated environments or include models without robust privacy protection. Given the highly intimate nature of transactional data, transparency around the information-handling practices of stablecoin-issuers will be of paramount importance in supporting end-user protections and trust.

The Group of Seven (G7), the International Monetary Fund (IMF) and the Bank for International Settlements (BIS) have jointed called for regulators to subject stablecoin-issuers to applicable data protection and privacy laws and regulations.[29] This goes beyond the issuer itself, as mere internal policy may be insufficient in providing adequate protection, given that many wallet operators in stablecoin ecosystems are third parties to the issuer and may have local legal obligations for data retention. This creates an accountability dilemma in stablecoin ecosystems, as well as the potential for stablecoin-issuers to adhere to robust privacy standards as issuers, yet also operate parallel business operations as wallet-providers according to differing standards.

The choice of third-party wallet-providers and other application-level developers or operators may also have an impact on trust in stablecoin networks and create confusion among consumers regarding accountability for their data and the consequences of data breaches. This risk is heightened in the context of stablecoins. Both a loss of trust in the issuer and a significant data breach of its ecosystem have the potential to result in a crisis of confidence among users, which could have a knock-on effect on a stablecoin's value and deposit-protection mechanisms.

Outside stablecoin ecosystems, a further risk to privacy has emerged in respect of surveillance by blockchain analysis companies. These are organizations that analyse on-chain transactions and can match such data with other publicly available data. A variety of cryptoasset ledgers are already under significant surveillance by such organizations[30]. Given the permanent nature of on-ledger transaction history and behaviours, the robustness of a stablecoin infrastructure against such surveillance will play a significant role in its ability to protect consumer data and privacy.

> Stablecoin-issuers will need to demonstrate a high degree of transparency and clarity in their data-handling practices and de-identification techniques

Given the highly sensitive nature of transactional data and ease of re-identification and external surveillance – plus the risk of a compounded effect on value of a loss of confidence resulting from, for example, a data breach – stablecoin-issuers will need to demonstrate a high degree of transparency and clarity in their data-handling practices and de-identification techniques, not only internally but in their wider ecosystems. Safeguards will need to be put in place in respect of external service providers and their ability to influence consumer sentiment, to prevent external risks affecting value. Stablecoin-issuers may also need to consider protective measures against external surveillance of their ledgers. For more detailed discussions on privacy-preserving technology, refer to the white paper in this series entitled Privacy and Confidentiality Options for Central Bank Digital Currency.

2.5 Security & technology risks

Several issues must be addressed with regard to how security protocols are designed, as well as how they are technically implemented. Poor technical design, such as bugs in smart contract code or poor security design choices, may also have a serious impact on consumers and expose them to loss.

Given that a detailed technical understanding of the systems underlying digital currencies will be beyond the average consumer, appropriate technical and audit standards may be necessary to neutralize technical impediments which can indirectly cause consumer risk. Nevertheless, the value of greater digital literacy among consumers should not be understated: it could play a significant role in helping consumers themselves to reduce the impacts of technical errors or issues. Policy-makers should consider the following issues:

- Variations in the digital literacy of consumers and how this may reduce or catalyse consumer risks
- How to standardize ways of conducting technical audits
- How to increase consumer understanding and transparency so that an informed choice is possible

2.6 Accountability risks

The identification of who is accountable to consumers for consumer risks is crucial and a core issue in respect of the consumer protections associated with stablecoin-issuers. Unlike traditional currency options, the decentralized architecture and governance models of digital currencies can make it difficult to find the right party to be accountable. Three primary instances emerge that require special consideration:

- Where decentralized architecture is used
- Where other consumers can influence rule changes
- Where issuers delegate responsibility of consumer engagement to wallet-providers and other VASPs

Decentralized architecture

Where a decentralized architecture is used for a stablecoin's protocols, particularly where rules (such as those governing reserves) can be altered after being set up by an issuer, there is the potential risk of a lack of a legal causal link with the stablecoin-issuer. The question arises as to whether a consumer would be able to hold such an issuer accountable in respect of losses suffered by the consumer resulting from such rule changes. Policy-makers will need to consider whether the policy imperative in relation to such issuers requires a form of legislated strict liability to hold issuers accountable to consumers in such instances.

Consumer ability to alter rules

Similar to the scenario above, a further question arises when consumers themselves are able to alter rules associated with the relevant stablecoin. Unlike e-money or cash, consumers may play a more active role in the process of creating and maintaining some stablecoins, in that they can propose and approve new governance rules. In this capacity, consumers act in a similar manner to shareholders of a company. Some mechanisms of company laws and securities laws, especially those designed to protect minority shareholders from infringement of majority shareholders, could be considered to protect consumer rights with respect to their roles in governance rules-making. Existing tort laws could provide some form of protection for consumers if the code-writers or issuers fail to honour their governance rules changes.

Delegation to VASPs

Many stablecoin-issuers that are not consumer-facing may take the approach of delegating consumer protection responsibilities to wallet-providers and other VASPs, which interact more directly with consumers. Policy and regulatory considerations will need to address such practices to ensure they do not result in supply-chain gaps in accountability to consumers.

3 Recommendations

The recommendations below include approaches and measures to improve consumer protection for different types of digital currency; they are primarily for the attention of policy-makers and regulators.

Same activity, same risk, same regulation

The regulatory approach to addressing the risks of digital assets should balance the need for both competition and innovation, and ensure a level playing field for all participants in the broader payments ecosystem. This is best achieved with the principle of "same activity, same risk, same regulation". Applying this principle would provide a consistent approach to consumer protection across the regulated and currently unregulated sectors, and would increase opportunities for both new and existing actors to provide safer and better services across the financial ecosystem.

> Consumer education needs to be carried out by neutral and trusted parties to ensure a consistent and objective approach, free of marketing influence

Consumer education

To minimize potential negative impacts of stablecoins on consumers and to enhance their wider adoption beyond simply facilitating payments for cryptocurrency trading, it is important to carry out consumer education to ensure people understand risks as well as their legal rights. Effective consumer education would include highlighting the different risks that stablecoins present compared not only to other stablecoins and digital currencies but also to existing currency options. Consumer education needs to be carried out by neutral and trusted parties to ensure a consistent and objective approach, free of marketing influence.

New or developed regulation and audit

Different types of reserve assets expose consumers to different types of risks. For stablecoins with fiat currencies as a reserve asset, they are exposed to risks related to reserve management along with potential inflation of fiat currencies and bankruptcy of deposit-taking institutions. There is also a transparency-related risk that consumers may have difficulty in verifying the existence of adequate reserves.

For stablecoins that choose cryptocurrencies as reserve assets, the risk lies in the price and fundamentals of the reserve cryptocurrency. Such a structure is similar to loans secured by publicly traded securities, which are considered a type of derivative under US laws. To ensure sufficient protection, the US margin loan laws and regulations require the underlying securities to have twice the value of the loan amount to allow sufficient room to absorb market shocks. Many stablecoins with cryptocurrency backing are overcollateralized; even so, given the often violent price swings in cryptocurrency markets, this overcollateralization still may not provide adequate backing.[31]

Limiting stablecoins to high-asset or high-income constituents or institutions may hinder the financial inclusion value proposition of stablecoins. Nonetheless, underserved populations are potentially at greater risk of inadequate understanding and consequent losses. Policy-makers can consider certain types of protections, including:

- Setting limits to the sizes of transactions and wallet balances, to limit the risk exposure of consumers
- Framing auditing and disclosure requirements to ensure the value of stablecoins is indeed what the issuer claims them to be; this could incentivize stablecoin-issuers to provide robust disclosure as a way to gain trust with individual consumers

Policy-makers may also need to consider how stable the value needs to be for a digital currency to qualify as "stablecoin" and what kinds of assets can be used as underlying assets. Depending on the risk level of different types of underlying assets, further consideration should be given to whether a given product is fit for the general public and what the appropriate transaction or balance limits should be. This risk-based approach could provide sufficient protection while not crushing innovation. There is also the question of where the reserve should be kept in order to provide sufficient protection and transparency, for example with central banks, commercial banks or digital currency exchanges.

Authorization and supervision

Firms that offer financial services or cash are often authorized and supervised by a local regulator, a central bank or an independent body. Historically these entities have generally been banks, but more recently payment and e-money institutions have been able to provide consumer-facing payment services.

As new firms come to market with a stablecoin offering, consideration should be given to the regulatory umbrella under which these services will be provided, as well as which functionaries will be responsible within this framework for the procedural implementation of regulations, authorization for certain activities and supervision. Stablecoin and CBDC services are often seen through the lens of the two-tier model of issuance and distribution. This gives rise to a number of activities that need to be considered for the purposes of consumer protection, such as those set out below:

Payment services

Firms that wish to provide consumers with payment services in stablecoins or CBDC should be authorized and supervised for the provision of such services.

Distribution

The appropriate regulatory framework for distribution will be different for CBDCs and stablecoins as outlined below.

For CBDCs, the distribution of central bank money might follow the current two-tiered structure, whereby access to central bank money is provided and made available via private-sector institutions (such as commercial banks). Policy-makers will need to consider possible future frameworks for such distribution and for new types of participants (e.g. non-banks such as VASPs), and whether new rules would be required to address varying risk profiles. Either way, the applicable supervisory regimes would need to apply proportionately to bank and non-bank firms that have access to central bank money in the form of a CBDC or that play a role in its distribution or custody.

Stablecoins will be distributed through models similar to those seen in e-money ecosystems, so current e-money legislation may be a suitable framework for such distribution. Where services are related to stablecoins, it would be appropriate to consider the need for additional operational risk or security requirements for the distribution of such stablecoins.

Custody

Requirements around the custody of a CBDC or a stablecoin is one of the most critical areas of regulation that will need to be clarified for consumer protection. For example, existing regulatory frameworks, such as the EU's PSD2,[32] do not currently apply expressly to custodial wallet services. Furthermore, while the European Commission's recent proposal to regulate markets in cryptoassets (MiCA)[33] would introduce requirements for custodians of private cryptoassets, it does not apply to the custody of a CBDC.

Ultimately, for a CBDC or stablecoin held in a digital wallet, the key management practices, security standards and ability of the wallet to support mixed payment functionality may all raise issues around the applicability of an existing regulatory framework to the custody of digital assets. Policy-makers will need to decide on a regulatory framework for custodial wallets with the necessary consumer and insolvency protections for such custody.

Conclusion

Consumers of digital currencies are not homogenous and vary significantly in risk profiles and tolerances, across both products and jurisdictions. Similarly, digital currencies, including stablecoins and cryptocurrencies, vary meaningfully in their setup, design and risk exposure. Although risks can be broadly identified, it will be up to policy-makers to match these to local market use cases to design or develop appropriate regulatory protections. What is clear is that such protections are indeed necessary. Stablecoins, the focus of this paper, introduce new opportunities but also new consumer risks into environments that are historically heavily regulated and centrally controlled.

At the same time, there is currently a lack of clarity around accountability and available options for redress. Solving this challenge will be one for policy-makers and stablecoin-issuers alike, and should be a priority as wider consumer adoption occurs. Designing an approach that allows for both innovation and experimentation in this new and growing industry,[34] while ensuring that consumers do not suffer undue or even catastrophic loss during the course of that experimentation, is a challenge that will require innovative modes of policy-making and public-private cooperation. In addition, consumer education will be a critical component in ensuring that consumers can make informed decisions that match their needs without exposing them to undue risk.

Endnotes

1. OECD, *Report on Consumer Protection in Online and Mobile Payments*, *OECD Digital Economy Papers No. 204,* 2012, http://dx.doi.org/10.1787/5k9490gwp7f3-en.
2. However, consumer protection issues exist, particularly for stablecoins, regardless of scale. See: G7 Working Group on Stablecoins, *Investigating the impact of global stablecoins*, October 2019, https://www.bis.org/cpmi/publ/d187.pdf.
3. G7 Working Group on Stablecoins, *Investigating the impact of global stablecoins*, October 2019, https://www.bis.org/cpmi/publ/d187.pdf.
4. Allen, Sarah et al., *Design choices for Central Bank Digital Currency: Policy and technical considerations,* Brookings Institute, Global Economy & Development Working Paper 140, July 2020, https://www.brookings.edu/wp-content/uploads/2020/07/Design-Choices-for-CBDC_Final-for-web.pdf.
5. "Stablecoins: Bridging the Network Gap Between Traditional Money and Digital Value – Brought to you by GMO Trust", *The Block Crypto*, 10 March 2021, https://www.theblockcrypto.com/post/97769/stablecoins-bridging-the-network-gap-between-traditional-money-and-digital-value-brought-to-you-by-gmo-trust.
6. G7 Working Group on Stablecoins, *Investigating the impact of global stablecoins*, October 2019, https://www.bis.org/cpmi/publ/d187.pdf.
7. A "participant of protocol governance" is a holder of a stablecoin who has the ability to vote on the protocols governing the stablecoin.
8. World Economic Forum, *Bridging the Governance Gap: Dispute resolution for blockchain-based transactions*, December 2020, https://www.weforum.org/whitepapers/93bd1530-0ded-48fa-8dee-e9b2d109d84d.
9. In this generalized example, we ignore more complex financial services and financial market complexities, even though these also form part of the traditional systems and stablecoin ecosystem alike.
10. "Countries Where Bitcoin Is Banned or Legal In 2021", *Cryptonews,* August 2021, https://cryptonews.com/guides/countries-in-which-bitcoin-is-banned-or-legal.htm. Note: the map in this article shows China as a country where bitcoin is legal – however on 24 September 2021, Reuters reported that China had banned all crypto transactions and mining, including bitcoin.
11. On 24 September 2021, Reuters reported that China had banned all crypto transactions and mining, including bitcoin. See: https://www.reuters.com/world/china/china-central-bank-vows-crackdown-cryptocurrency-trading-2021-09-24/.
12. Schonberger, Jennifer, "Treasury looks at run risks in stablecoins, pushes for new rule proposals", *yahoo!finance*, 15 September 2021, https://news.yahoo.com/treasury-looks-at-run-risks-in-stablecoin-pushes-for-new-rule-proposals-193053375.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAKDA7qtrvFXvWYRrjcUwiDHw2igO3ugCjzN5vnjDli2_NOYQNFoPdvdl3TRC9DFZVkyT1ebHZf1GNixPt4HPkGE3DgpCHj6m78uCkrOm0iM85MYN0vrhXuFzLXXxYMv0lMMuV4d-ltUFx9XRmqFZl-rpmQ3ZOtkzuf9s0kF1KjMa.
13. For example, see:

    1) "Reserves Breakdown at March 31, 2021", *Tether,* https://tether.to/wp-content/uploads/2021/05/tether-march-31-2021-reserves-breakdown.pdf.

    2) "Independent Accountant's Report: To the Board of Directors and Management, Tether Holdings Limited", *Moore Cayman,* 6 August 2021, https://tether.to/wp-content/uploads/2021/08/tether_assuranceconsolidated_reserves_report_2021-06-30.pdf.

    3) "Attorney General James Ends Virtual Currency Trading Platform Bitfinex's Illegal Activities in New York", *Letitia James, NY Attorney General,* 23 February 2021, https://ag.ny.gov/press-release/2021/attorney-general-james-ends-virtual-currency-trading-platform-bitfinexs-illegal.
14. For example, see:

    1) European Commission, *Proposal for a Regulation of the European Parliament and of the Council on Markets in Cryptoassets, and amending Directive (EU) 2019/1937,* 24 September 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593.

    2) Singapore Government, *Payment Services Act,* 14 January 2019, https://www.mas.gov.sg/regulation/acts/payment-services-act.
15. For example, cryptocurrency-backed stablecoins bear a far greater risk than stablecoins backed using reserves or central bank RTGS accounts.
16. For example, see Minwalla, C., "Security of a CBDC", *Bank of Canada*, June 2020, https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-11/.
17. Referred to by the European Central Bank (ECB) as "tokenised funds" in: Bullmann, Dirk et al., *In search for stability in cryptoassets: are stablecoins the solution?,* European Central Bank, 2019, https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf.
18. It should be noted that there is always a potential risk of a run on a traditional currency, although this is not specifically mentioned.

19. The definition of e-wallet here includes e-wallets that rely on SMS messaging and app-like e-wallets.

20. Oliveros, Rosa and Pacheco, Lucia, *Protection of Customers' Funds in Electronic Money: a myriad of regulatory approaches*, BBVA Research, 28 October 2016, https://www.bbvaresearch.com/wp-content/uploads/2016/10/Safeguardingelectronicmoneyfunds_en.pdf.

21. Ehrentraud, Johannes, et al., *Policy responses to fintech: a cross-country overview,* Bank for International Settlements, January 2020, www.bis.org/fsi/publ/insights23.pdf.

22. Oliveros, Rosa and Pacheco, Lucia, *Protection of Customers' Funds in Electronic Money: a myriad of regulatory approaches*, BBVA Research, 28 October 2016, https://www.bbvaresearch.com/wp-content/uploads/2016/10/Safeguardingelectronicmoneyfunds_en.pdf.

23. "The Direct Debit Guarantee: What Does it Really Mean?" *ClearDebit*, 18 February 2013, https://cleardirectdebit.co.uk/the-direct-debit-guarantee-what-does-it-really-mean.

24. European Commission, *Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937*, 24 September 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593.

25. "Electronic money token" or "e-money token" means a type of cryptoasset 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.

26. European Commission, *Payment services (PSD2) – Directive (EU) 2015/2366*, 12 January 2016, https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en.

27. HM Treasury, *UK regulatory approach to cryptoassets and stablecoins: Consultation and call for evidence,* January 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950206/HM_Treasury_Cryptoasset_and_Stablecoin_consultation.pdf.

28. "Deep Dive: The Benefits And Challenges Of Real-Time Push Payments", *PYMNTS.com*, 26 September 2019, https://www.pymnts.com/news/faster-payments/2019/benefits-challenges-real-time-push-payments-pull/.

29. G7 Working Group on Stablecoins, *Investigating the impact of global stablecoins*, October 2019, https://www.bis.org/cpmi/publ/d187.pdf.

30. Powers, Benjamin, "'Digital Mercenaries': Why Blockchain Analytics Firms Have Privacy Advocates Worried", *CoinDesk*, 14 September 2021, https://www.coindesk.com/tech/2020/11/04/digital-mercenaries-why-blockchain-analytics-firms-have-privacy-advocates-worried/.

31. As was experienced with MakerDAO's DAI when the price of the cryptocurrency ether (ETH) rapidly fell in March 2020, despite DAI being pegged 1:1 to the US dollar and over-collateralized with ETH.

32. European Commission, *Payment services (PSD2) – Directive (EU) 2015/2366,* 12 January 2016, https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en.

33. European Commission, *Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937*, 24 September 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593.

34. "Top Stablecoin Tokens by Market Capitalization", *CoinMarketCap*, https://coinmarketcap.com/view/stablecoin/. As of 19 October 2021, the market capitalization for stablecoins had reached over $130 billion.

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org