International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

FG-DFC

(06/2019)

ITU-T Focus Group Digital Currency including Digital Fiat Currency

Regulatory Challenges and Risks for Central Bank Digital Currency

Regulatory Requirements and Economic Impact Working Group

Focus Group Technical Report

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The procedures for establishment of focus groups are defined in Recommendation ITU-T A.7. TSAG set up the ITU-T Focus Group Digital Currency Including Digital Fiat Currency (FG DFC) at its meeting in May 2017. TSAG is the parent group of FG DFC.

Deliverables of focus groups can take the form of technical reports, specifications, etc., and aim to provide material for consideration by the parent group in its standardization activities. Deliverables of focus groups are not ITU-T Recommendations.

Regulatory Challenges and Risks for Central Bank Digital Currency

About this report

This report was written by Rohan Grey, Cornell School of Law with inputs from the Regulatory Requirements and Economic Impact Working Group of the ITU-T Focus Group Digital Currency including Digital Fiat Currency.

The author acknowledges the contributions and feedback received from members of the Regulatory Requirements and Economic Impact Working Group. The following input documents were drawn upon and incorporated into the following report:

- Cooper, B., Esser, A., & Allen, M., 2019. "The Use Cases of Central Bank Digital Currency for Financial Inclusion: A Case for Mobile Money", The Center for Financial Regulation and Inclusion. (https://cenfri.org/wp-content/uploads/2019/06/CBDC-and-financial-inclusion_A-case-for-mobile-money.pdf) [DFC-I-034R1];
- Cooper, B., & Allen, M., 2018. "DFC in the Common Monetary Area: Feedback From the Regulatory Requirements & Economic Impact Survey: Legal Frameworks". Center for Financial Regulation and Inclusion;
- Dharmapalan, J. & McMahon, C., 2015. "The Case for Digital Fiat Currency: Central Bank Issued Digital Currency and its Impact on Financial Inclusion". eCurrency;
- Deshpande, M., 2018. "Government as User of DFC". FG-DFC WG I Input Document;
- Dong, R., 2018. "Monetary Policy Implications". FG-DFC WG I Input Document;
- Grey. R, 2017. "Macroeconomic Policy Implications of Digital Fiat Currency". eCurrency. [DFC-I-023];
- Helmy, M., 2019. "Inclusion Through Digital Financial Services and Fintech: The Case of Egypt". FG-DFC WG I Input Document; Hutabarat, A., 2018a. "Monetary Policy Implications of Digital Fiat Currency". FG-DFC WG I Input Document;
- Hutabarat, A., 2018b. "Unintended Consequences and Possible Risks: Key Concerns and Possible Mitigation Strategies", FG-DFC WG I Input Document;Meaning, J., Dyson, B., Barker, J., & Clayton, E., 2018. Broadening Narrow Money: Monetary Policy With a Central Bank Digital Currency. Bank of England Staff Working Paper No. 724. (https://www.bankofengland.co.uk/-/media/boe/files/working-paper/2018/broadening-narrow-money-monetary-policy-with-a-central-bank-digital-currency.pdf);
- Ndung'u, N., 2018. "Payment Systems and DFC". FG-DFC WG I Input Document [DFC-I-029R1];
- Realeboha L., 2019. "DFC in a Common Monetary Area," Bankers Association of Lesotho. FG-DFC WG I Input Document [DFC-I-037Rev1];
- Said, A., 2019. "The Economic Impact of Digital Fiat Currency: Opportunities and Challenges". National Telecom Regulatory Authority of Egypt. FG-DFC WG I Input Document;
- Sathnur, A., 2018a. "Creation of Ideologies and Concepts for Possible Economic Benefits and Impact of DFC on Mobile Payment Ecosystem". FG-DFC WG I Input Document;
- Sathnur, A., 2018b. "Creation of Ideologies and Concepts for the Social & Practical Externalities: Privacy Implications, AML Opportunities and Risks, Environmental Impact of DFC in Reducing the Production of Cash and Coins". FG-DFC WG I Input Document;

- Tak, A. & Gupta, M., 2019. “United Payment Interface (UPA): India Case Study and User Experience”. Ministry of Communications, India. FG-DFC WG I Input Document [DFC-I-036].

It is understood by members that this document describes an evolving field of study and practice. Definitions of terms and descriptions of considerations should thusly be taken as best thinking by authors at date of publication. Authors point readers to complementary work issued by this Focus Group and recommend updated thinking, issued after point of publication, to inform a comprehensive understanding of the topic and key considerations.

If you would like to provide any additional information, please contact Vijay Mauree at tsbfgdfc@itu.int

Table of Contents

1. Overview

The rapid growth of the Internet and digital technology has affected all economies, whether emerging or developed, across the world. The financial sector has been directly influenced by technology due to the growth of electronic commerce and electronic payments. The emergence of digital currencies such as Bitcoin and the underlying blockchain as well as the distribution ledger technology have attracted significant interest. These developments have raised the possibility of considerable impacts on the financial system and perhaps the wider economy.

As a result, over the past few years, public authorities and central banks around the world have been monitoring developments of digital currencies and studying their implications. A question that has been raised frequently is whether central banks themselves should issue digital currency that could be used by the general public or not. The legal status of cryptocurrencies was always in question. Some administrations have banned them and other had implicit bans. In many other countries they are still under study and only official warnings from using and investing in cryptocurrencies were announced.

The huge price leaps that happened to Bitcoin towards the end of 2017 until it reached its highest ever price, (19000 USD) since the beginning of its trading, followed by the significant fall that took place afterwards till it fell under the level of 4000 USD in 2018, made the Central banks more worried about the future of this market.

In addition to that, the increase of developing new cryptocurrencies as well as the lack of control over it, made the central banks very alert to the futuristic view of this sector keeping their eyes wide open to this rapid growth.

The idea of issuing central bank digital currency, or Digital Fiat Currency (DFC),[1] has been studied by central banks in order to offer a formal/legal substitute for the consumer that is trusted and protected by central banks. Refocusing policy attention away from private cryptocurrencies and towards a publicly-issued DFC will enhance the suite of financial inclusion tools that are already in place, offer "cash"-only households a leap into digital transactions, and increase the consumer choices of how to manage their household income and expenditures.

DFC is, at its legal core the digital equivalent to physical currency. There are two broad approaches to implementing a DFC system: a direct access approach through accounts at the central bank, and a token approach through in independent wallet network. These models could be adopted separately, or combined in a hybrid approach.[2]

Account approach: Through this approach, the central bank will need to give every citizen a DFC account and this would also imply providing the citizens with sort codes, account numbers and payment cards so that the money in those accounts could be used. In addition, customers would need a way to check their balance and transactions, so internet or mobile banking would be a minimum requirement, and telephone banking would be necessary for some account holders. Central banks

[1] For the purposes of this document, the terms 'CBDC' and 'DFC' are used interchangeably, however according to the taxonomy provided in Doc 44], the term 'DFC' can be broader, encompassing a wider range of potential institutional arrangements.
[2] This categorization is intended only as a broad framing, it is not the only way in which different DFC models could be classified. Indeed, depending on context, certain models, such an open, permissionless, distributed-ledger-based model, could be described as either a token or account based system. Nevertheless, for introductory purposes, this distinction is still useful.

could manage accounts on behalf of customers directly, or alternatively, could delegate responsibility for account management to third parties.
Indirect Access Approach: In this approach DFC, units are issued by the central bank via a dedicated DFC payments platform, they can be converted into bank deposits and other forms of government–issued liabilities, including physical currency, central bank settlement balances (reserves), and interest–earning government securities. Transactions and cash storage are conducted via DFC wallets or applications, which are hosted and managed by licensed financial intermediaries, but remain to be the property of the wallet– or application–owner. Also all customer service activities are going to be handled by the intermediaries.

A proper designed indirect DFC system should have at least the following characteristics:

a) The central bank is the sole authorized party to issue DFC liabilities, with similar ownership restrictions and legal tender protections as physical currency.

b) The central bank guarantees the convertibility of DFC to physical currency.

c) Financial intermediaries that meet basic criteria are eligible to apply for a special DFC intermediary license, and, upon receipt of such a license, are eligible to establish and maintain DFC wallets on behalf of retail customers, and to convert, upon demand, currency and/or government–guaranteed obligations, at face value, into DFC units.

d) Any individual or entity can obtain a DFC wallet managed by a licensed DFC intermediary, and store funds in that wallet, without technical limit.

e) Licensed DFC intermediaries can make payments from customers' DFC wallets, on their behalf, through a trusted DFC intermediary network, mediated and backed by the central bank.

2. DFC Efficiency and Costs

1. Reduction of Usage of Cash and Coins

Switching to a digital fiat currency system has the potential to improve efficiency and generate savings through reducing reliance on cash and coins, and allowing the biophysical and human resources currently devoted to maintaining those systems to be redirected elsewhere.

However, responsible and inclusive digital payments ecosystems are not a monolithic, one-size-fits-all equation. Unlocking the power of digital payments in any given country requires a strategy tailored to specific national conditions and market characteristics.[3]

2. Research and Diagnostic Methodologies

Today, a range of diagnostic tools are emerging that can give policymakers a significant head start. A leading example is the methodological framework recently developed by the World Bank to measure retail payment costs and compare them across payment instruments and across countries. This methodology has been applied with significant success in Albania, yielding valuable data that can inform policy choices about the most effective payment instruments for such countries. The Bank of

[3]For more, see Realeboha (2019).

Canada has also carried out a similar study to estimate the cost of point-of-sale payments in the country, producing valuable data for policymakers.

In addition, and importantly for policymakers, the World Bank methodology produces valuable data about who bears the costs of existing payment instruments. In particular, such studies highlight the significant costs of paper-based or physical payment instruments.

Survey results and conclusions from these methodologies can hence become important pillars of policy design and implementation, providing a strong evidence base about costs and potential benefits. In doing so, methodologies for assessing the cost of payment instruments can support the development of payments infrastructure and be an enabler of market development – a critical factor in expanding digital payments ecosystems to meet user needs, thus driving financial inclusion.

It's no secret that surveys can be expensive. However, the ready availability and applicability of this type of cost assessment methodology can substantially reduce costs, with a very strong prospect of generating valuable data. Furthermore – with methodologies already identifying potential savings around 1 percent of GDP – the value and the benefit of policy incentives from these methodologies tend to speak for themselves, and in any case, vastly outweighs any survey costs.

Transitioning toward digital payment systems and instruments can meaningfully enhance economy-wide efficiency. However, the data resulting from these cost assessment methodologies should be used in conjunction with existing knowledge products and foundational principles for digitizing payments.

3. Sample Findings

A brief snapshot of findings in Canada and Albania provides a good sense of the value of these studies and the data they are able to generate. The study carried out by the Bank of Canada shows the total resource costs of payments instruments stand at 0.78 percent of GDP; the costs of point-of-sale payments in cash are a staggering 0.45 percent of GDP; and the costs of cash increase with the size of transactions. In Albania, a study using the World Bank methodology puts the costs of paper-based instruments – that is, cash and checks – at roughly 2 percent of GDP. The methodology shows that this cost could be halved by migrating just 70 percent of payments to digital channels. For low-income pensioners, consumers, governments, and payment providers, the potential savings are enormous.

For example, for paper-based instruments in Albania, 50 percent of the costs are borne by consumers, 25 percent by businesses, 24 percent by payments service/infrastructure providers, and 1 percent by government agencies. With electronic payments, 55 percent of costs are borne by payment service/infrastructure providers, 30 percent of costs are borne by consumers, 14 percent of costs are borne by businesses, and 1 percent is borne by government agencies.

4. General Recommendations

To maximize efficiency and cost benefits, efforts to digitize payments should focus on four areas:

- Connectivity: Mobile phone and internet connectivity helps ensure digital payment ecosystems develop in an inclusive way that also allows the digital payments ecosystem to be scalable

Interoperability: Across payment platforms, interoperability underpins efficiency, competition, and accessibility, helping to drive usage and thus increase market size and lower unit costs.
Electronic Personal Identification Systems: These identification systems can help ensure user protection, enable innovation to drive new capabilities, and expand digital ecosystems responsibly. Additionally, consolidated national databases and advanced biometrics can boost the confidence of users, investors, and policymakers.
Regulatory and Institutional Capacity: This capacity supports market innovation and ecosystem growth while also ensuring that growth is inclusive, responsible, and sustainable, including through thoughtful regulation.

Possibility for Further Study: Beyond this report, ITU-T SG3 could conduct further study of the introduction of DFC to be used on the mobile financial services platforms and their interoperability aspects. In addition to that SG3 could assess the impact on the regulatory environment when introducing DFC, and also the level of involvement needed by the telecom regulator.

3. Monetary Policy Implications

1. New Universal Public Instrument

Digital Fiat Currency technology has the potential to simplify the public finance ecosystem by consolidating different categories of publicly issued obligations (from central bank reserves to physical cash to treasury or agency securities) into mere variations of a new, safe, generally interoperable DFC instrument. Such an instrument could easily be programmed with different information, such as the issuing agency, maturity, yield, and convertibility rates and conditions, and could be traded and transmitted across a common payments platform running across the entire administrative state, thereby opening up new opportunities for monetary policy implementation.

2. Revised Treasury-Central Bank Dynamic

The introduction of a DFC platform would be an opportunity to revisit the current method of central bank-treasury coordination in the conduct of monetary policy, and allow for a revised approach that reduces the need for close daily coordination between treasury debt managers and the central bank in the administration of monetary policy, as well as clarify the political and operational boundaries between monetary and fiscal policy.

3. Expanded Central Bank Balance Sheet Access

A DFC system has the potential to expand the range of financial institutions and actors with direct access to the settlement and liquidity services of the central bank’s balance sheet, including mobile money operators. This, in turn, would affect the daily provisioning of market liquidity as part of monetary policy implementation, providing greater flexibility and operational tools than before.

In particular, a DFC system may increase the need for the central bank to supply liquidity during turbulent times. If these challenges are overcome, one possibility is that the central bank eventually becomes a liquidity provider of last resort in times of crises. However, care must be taken to ensure such widespread liquidity provisioning does not result in a destablization of the currency.

4. New Financial Institutions

A DFC system may generate new markets and commercial opportunities that justify the creation of new categories of financial institutions, licenses, or corporate charters, which will in turn need to be incorporated into existing monetary policy implementation frameworks. These could include narrow

banks, e-money transmitters, mobile money operators, or other forms of money market institutions and wallet-managing intermediaries. In particular, a ‘wholesale CBDC' could be used as a settlement asset in financial markets by firms that do not currently have access to central bank reserves (Bech & Garratt, 2017). In addition, there is potential for particular technologies within the DFC ecosystem, such as QR codes, to expand the range of financial products and services available to non-bank financial institutions and/or businesses, which could also have an economic impact on the cost of doing business, as well as the range of actors involved in particular financial markets.[4]

5. Depositor Outflow

In the current banking system, commercial banks create reserves indirectly by issuing loans.A retail CBDC which is accessible by households directly could thus change the dynamics of the money creation process, while also allowing for P2P loan to gain greater prominance. However, the credit risk exposure of these new channels of money creation could be significant. Moreover, the traditional commercial banking system could be threatened, as their role as agents of the central bank may become less systemically important.

The introduction of greater interoperability and safety of mobile money and/or money transmitter services may encourage higher rates of depositor outflow from banks, thereby reducing the availability of relatively cheap depositor funding for the banking system. However, any systemic effects of depositor outflow on the cost of bank liquidity can be countered or effectively neutralized, however, by encouraging greater use of the discount window and provisioning of cheap, collateral-based liquidity to broader financial markets, as well as one-time swaps between private and public monies.

6. New Policy Levers

Monetary policy mainly focuses on two core functions – varying the quantity of different forms of government and central bank-issued liabilities in circulation, and adjusting the interest rates paid on those liabilities. These functions are achieved through different tools, including buying or selling different kinds of securities, changing the discount or interest rate paid on or against different classes of assets, and changing the amount of settlement reserves banks are required to hold against their assets.

The introduction of digital fiat currency opens up the possibility of new channels for monetary policy implementation, including levying positive and negative nominal interest rates directly onto retail depositor accounts, establishing a universal, publicly-guaranteed payments system for both retail and wholesale depositors, and consolidating various forms of government-guaranteed liabilities into subvariants of a common DFC instrument. It will be important to evaluate both the potential and limits of such levers, as well as consider how they interact with the existing monetary policy framework.

In particular, interest rates could be used to stabilize inflation and output, as the primary instrument of monetary policy, or it could be used to regulate demand for CBDC. Alternatively, a non-interest-bearing CBDC could be considered closer in spirit to central bank notes. If a CBDC accrues interest, it will be an instrument that needs to be incorporated into the monetary policy implementation framework, otherwise it is just a payment factor which works outside the monetary system, just like

[4]For more, see Realeboha (2019).

"e-cash".[5] According to Sweden Riksbank's report of the e-krona project in 2017, an e-krona that does not accrue interest could in other words mean that the lower bound is adjusted upwards, closer to zero, while an e-krona with a negative interest rate would retain the possibility of a negative policy rate.

7. New Opportunities/Challenges for Financial Stability

DFC technology has the potential to transform the public financial landscape, as well as the banking system and related payments systems. It will be critical to assess the financial stability risks posed by fraud, underregulation and lack of supervision, in order to ensure that monetary policy does not exacerbate or otherwise obscure potentially destabilizing private sector dynamics.

8. International Dynamics

The development of global DFC technology will require technical standards harmonization across jurisdictions, as well as the establishment of new clearing and settlement platforms. Such efforts can and should be coordinated with international technical standards-setting for global telecommunications hardware and software, including cell phones, routers, SIM cards, and QR codes.

While real-time, cross-border payment settlement is the future, today the primary concern of policymakers is crisis prevention. Use cases vary by individual countries' situations. Developing countries in particular must be careful when trying to issue a CBDC that has cross-border transaction functions. For example, China has banned fiat to cryptocurrency trades in order to prevent fiat currency outflow, which in turn would have generated exchange rate pressure in the event of a substantial decline in foreign reserves.

9. Cross-Border Payments

There is a spectrum of different kinds of cross-border payments that will likely be implicated by the adoption of a DFC system:

Cross-Border Payments Between Consumers/Firms: such transactions could be either based on P2P wallets, intermediaries with accounts in multiple jurisdictions, or multinational transactional networks based on correspondent banking arrangements

Intra-Firm Transfer of Funds: this could be either multinational firms with registered DFC accounts in multiple banking jurisdictions, or via multinational banking institutions with local subsidiaries in multiple jurisdictions/connected to multiple central banks.

Removing Funds from Issuing Jurisdiction: this could take place by transferring domestic currency held in a wallet to another wallet managed outside of the issuing country's jurisdiction

Cross-Border Securitization of Domestically Held Funds: for example, by establishing foreign claims over balances held domestically, or income streams from assets retained domestically by a third party

Convertible and/or Local Currency Denominated Foreign Instruments: for example, creating a domestic instrument whose value is linked to the value of a foreign currency.

10. Global Currency Network Design

DFC systems have different cross-border dynamics and jurisdictional implications depending on design choices. In addition, regulatory dynamics will differ depending on whether DFC is implemented only in one country, or in both/all countries involved in bilateral/multilateral

[5] Meaning et al (2018).

transactions, as well as whether such transactions occur against the backdrop of a global DFC regime, via harmonized DFC domestic standards and/or a global eSDR based on DFC architecture/principles.

Account vs Token-Based Systems

Account-based DFC systems are centered around the jurisdiction of the account-managing intermediaries. For example, domestic interbank settlements are presently settled via changes made to accounts represented on the central bank's balance sheet, which is hosted on a domestically-located computer server. Furthermore, balances transferred may be subject to clawback and other rules to prevent fraud and theft.

By contrast, token-based DFC systems are centered around individual user wallets, which may be located on servers that are physically hosted outside of the relevant country. Furthermore, funds considered legally to be 'currency' will typically be considered property of the 'current' owner, absent specific circumstances.

Registered vs. Unregistered Systems

Registered DFC intermediary systems are easier to regulate, as the relevant jurisdiction can enforce its laws at the point of registration.

By contrast, unregistered or 'open' intermediary systems must rely on enforcement via international standards/protocols, combined with domestic law enforcement in the relevant jurisdiction.

Real-Time vs Delayed-Time Settlement

The relevant payments law principles that apply to a DFC system will depend in part on whether it is a live-time, gross settlement based system, or a delayed, batching-based settlement system.

11. Monetary Union Dynamics

DFC systems will also need to consider the unique needs and challenges of implementation within a monetary union in the absence of a single, common political and/or fiscal authority (such as the European Union).

This includes as a threshold matter the capacity of individual nations to implement DFC domestically within an existing currency union. In the absence of specific enabling legislation at the supra-national level, or coordinated between nations, this will likely require that DFC be adopted on the basis of existing frameworks of monetary and payment law and regulation.

It also includes national-level policy considerations in the event of a union-wide adoption of DFC. For example, countries will have to consider the implications of having a national central bank capable of issuing currency that is pegged to the common union-wide standard. Under such a system, each country is able to retain its independent monetary authority, but the management of its currency, as well as foreign exchange market dynamics, are subject to the policies and regulations of the monetary union as a whole.

The potential for DFC within a monetary union depends on the definition and stipulated requirements of the common unit of account and legal tender, as well as the legal capacity of sovereign nations within the union to establish and regulate national legal tender within their own respective territories, as well as recognize domestic legal tender issued by other nations within the union.

It also depends on the legal and institutional structures underpinning at-par convertibility between liabilities issued by different subnational actors and their central banks (including currency and government securities), as well as the rules and conditions of inter-national central bank settlement, reserve requirements, and liquidity provisioning within the currency zone.

It is likely that a DFC system would be established initially as part of a cross-border interbank payments solution before its benefits were extended to domestic retail purchases given the specific liquidity and reserve dynamics of a currency union, which resemble those of a pegged exchange rate regime. Hence, intra-union coordination and harmonization is critically important.

The development of circular, guidance notes or practice notes may be the most efficient method of providing regulatory guidance if to avoid the protracted nature of regulation and legislation amendment procedures. Regulatory sandboxes, in one primary jurisdiction, may additionally assist monetary authorities to develop their understanding and regulatory provision for DFC. Once successful, these sandboxes may be applied to the rest of the union for the potential implementation of DFC.

For an example of an in-depth analysis of the legal and regulatory issues associated with adoption of DFC in the context of a monetary union, see Cooper & Allen (2018).

4. Social and Practical Externalities

1. Environment

DFC technology has the potential to have a positive environmental impact, by reducing reliance on non-renewable physical instruments made from paper and/or metal for daily retail payments, as well as reducing the energy costs of existing digital payments infrastructure, including both public and private payments systems.

However, the technical architecture and requirements of DFC systems should consider the costs of greater reliance on scarce or precious metals or other elements, both in core payments system hardware, and any subsidiary/supporting infrastructure, in addition to the benefits of reduced reliance on physical notes and coins.

At the same time, it is important to preserve physical payments media in the event of digital system failure, which will require ongoing investment into basic physical instrument-enabling infrastructure. Certain kinds of digital technology may work offline as well as online, requiring appropriate battery and near-field communication technology integration.

2. Privacy

Security of financial data is highly important due to its sensitive and potentially valuable nature. In particular, one issue to be addressed is the classification of particular transactional data as personal or private data, and the appropriate restrictions on usage of such data by the government, payments intermediaries, or third parties.

Similar privacy considerations apply to identity-related data. When a new digital money account is opened, certain information is requested from the account holder. Certain norms are to be followed during this account opening procedures. Data collection would be private and protected as the supplied data would be under the norms of data privacy and data protection, aiming to achieve a total 100% of “no – misuse clause” of this information.

With the rise of digital fiat currency technology it may be necessary to establish protocols to maintain or preserve physical cash as an alternative form of payment, to prevent the loss of an anonymous/offline alternative to digital payments. At the same time, the introduction of new digital fiat currency technologies and platforms may require a more systemic rethinking of digital privacy standards and regulatory requirements, as differences between existing technological silos are dissolved and a new regulatory and technical architecture emerges.

This new architecture will be comprised of distinct technical and legal layers, that together comprise the DFC ecosystem. Each layer will include its own security elements, in addition to system-wide and intermediary-specific requirements. In addition, certain legal compromises and standards may have to be renegotiated in light of modern technological capacities, and the new legal and political risks presented by big data and surveillance analytics. Moreover, many financial and commercial trading and settlement systems will integrate or build upon the DFC platform, thereby requiring harmonization between DFC security and privacy standards and those of other markets.

A privacy and security framework will need to balance different tensions and interests, including between government, payments system intermediary, account/wallet-managing fiduciary, and/or consumer. The broad social implications of digital technology necessitates that privacy issues, including the appropriate balance between anonymity and law enforcement, should be deliberated publicly and openly, with solicitation of input and perspectives from a wide variety of stakeholders and interest groups.

3. Consumer Protection

Good consumer protection practices protect the interests of consumers, creating trust in using digital financial services (DFS), while preserving the commercial incentive to provide these services at scale. Developing a regulatory framework requires regulators to analyze the roles of players in the value chain (banks, MNOs, non-banks, agents, e-money issuers, etc.) and consumer risks. Digital financial services in many emerging economies are driven by innovations in mobile technologies, so the mobile network operators that provide the telecommunications infrastructure are critical players in the ecosystem.

Consumers can experience a number of potential risks when conducting DFS transactions. Fraud is an example of the various forms these risks can take. For example, DFS provider employees, may gain access to consumer accounts and use the private information for dishonest purposes, or fraudsters may use social engineering scams to obtain money or information from unsuspecting customers. Consumers can also experience fraud from agents, who could charge them unauthorized fees, or access private customer information including their PINs.

The DFS provider is the entity which is actually providing the service to the consumer and is ultimately responsible for ensuring transparent, fair, and safe services and protecting the consumer's funds and personal information. For instance, clear terms and conditions in the DFS service contract explaining the consumer rights and obligations, clear explanation of fees charged to consumers, the availability of timely complaint mechanisms and dispute resolution process reduces risk while enhancing consumer trust in using DFS. The liability of consumers, agents and DFS providers in case of errors is also an important part of transparency. Four core themes were identified as central to consumer protection in order to mitigate the risks for consumers.

a) Provision of information and transparency
a) Dispute resolution
b) Fraud prevention
c) Data privacy and protection

With respect to Digital Fiat Currency (DFC) in particular, intermediaries will likely have to comply with some combination of money transmitter and banking regulatory requirements, given the hybrid nature of wallet-management and DFC payments. It will also be important to maintain hardware and software security standards for approved intermediaries given the potential for security breaches to extend across platforms as a result of DFC's inherent interoperability.

In addition, DFC consumer protection considerations extend beyond financial service provisioning to the broader telecommunications and data-network practices in which DFC systems are embedded. This includes concerns regarding mobile phone hardware, data-gathering and data-sharing between financial and other mobile services, integration between mobile wallets and other account-based digital services, etc.

As financial technology or 'fintech' companies become increasing indistinguishable from broader 'tech' companies, and as existing platforms such as Google, Apple, and Facebook expand more directly into financial services, it is likely that consumer protection will become increasingly integrated and holistic, requiring coordination of efforts and expertise between different agencies and actors responsible for the financial and IT sectors.

Possibility for Further Study: Beyond this report ITU-T SG3 could study the policy aspects related to consumer protection in a DFC system.

4. Hacking and Cybersecurity

In addition to concerns regarding individual privacy and protecting abuse of personal financial data by public authorities, DFC regulators must also address risks of hacking by third-parties. This requires strong technical security standards, auditing and resolution systems, and robust and effective regulatory and law enforcement.

In particular, cybersecurity is of prime importance to preserving financial privacy under a DFC system. It is possible that data privacy and data protection guidelines could be achieved by utilizing the technologies of Artificial Intelligence and Neural Networks, such that ethical or unethical hacking by illegal interventions would be deciphered by neural networks algorithms by deriving certain patterns of logging into the DFS systems.

5. Governments as DFC Users (vs. Issuers)

1. The Role of Government With Respect to Currency

Governments typically have two distinct functions as far as currency is concerned. First is the Monetary Function associated with currency issuance, interest rate setting, and liquidity management that usually vests in the Central Bank. Second is the Fiscal function associated with spending, taxation, and issuance of government securities that is carried out by Central/Federal government. The fiscal actions of the government tend to have direct impact on the overall macro-economic framework and livelihood of the population, thus it is necessary to assess the impact of Governments using DFC.

2. Government Spending and Economic Activity

Any Government setup (Central/Federal and provincial taken together) is involved in a significant way in a particular economy, irrespective of level of development. This tends to increase if the Government also runs Public Sector Industries. The total expenditure by Governments as percentage of GDP for G20 economies varies from 20% to a staggering 60%. While the relative spending may vary significantly, government by far is the single largest spender, in any economy. Similar to being highest spenders, Governments also tend to be the institution with highest earnings.

While being the largest single economic actor, Governments have ubiquitous presence i.e. every single economic entity whether individual or institutional transacts with the government both ways. Therefore, the Governments using DFCs will have far reaching impacts. These are discussed as benefits and concerns.

3. Digitizing the Economy

The world has witnessed communication revolution through the penetration of mobile telephony. For the governments to use DFC for payments, investment in new technologies and up-gradation of existing infrastructure will be necessary. This investment would create positive externalities for other aspects of Governance, extending beyond mere payments. The ease of money-flow to and fro Government could be utilized to overhaul the governance apparatus substantially. Enhanced digital connectivity acts as catalyst for economic growth. The World Bank estimates that 10% increase in broadband penetration increases the GDP of developing countries by 1.38%. DFCs being transferred over mobile platform could provide a full-fledged rollout of smart phone and app based service delivery platforms, particularly in those areas where the costs of setting up physical infrastructure are prohibitive. Widespread use of DFCs by Government will also create more visibility and transparency in informal economy, extending the benefits of social security schemes to the marginalized workers. It also has the potential to enhance the process of digitization of the economy.[6]

4. Government Payments

Developing or Developed, Governments tend to shift towards Digital Payment solutions in order to prevent pilferage and misuse of public funds. The World Bank in its 'Digital Dividend 2016 report' mentions that India alone could save as much as $11 Billion in subsidies through the *Aadhar* (Unique Identification Number) based digital payment systems.

The advantages of moving towards Digital Payments are more pronounced in developing and least developed economies, where a significant section of the population is dependent on social security measures. While 2 billion people do not have a bank account globally, more than 40 percent of the world's population has access to the Internet, with new users coming online every day. Among the poorest 20 percent of households, nearly 7 out of 10 have a mobile phone. The poorest households are more likely to have access to mobile phones than to toilets or clean water.

In addition to promoting digital financial inclusion, DFCs could possibly eliminate the traditional payments intermediaries (including Commercial Banks), providing faster and cheaper money transfer. In addition, social security benefits transferred through DFCs could also be made conditional – i.e. DFCs that will be usable only to purchase food or medical services etc – thereby improving data collection and monitoring.

5. Public Transparency

The Governments are the custodians of Public Money with a fiduciary responsibility to use it appropriately. Expansive institutionalized mechanisms for auditing the government revenues and expenditures exist worldwide. With the Governments using DFCs, auditing and detecting the misuse will become easier. DFC ecosystem could potentially preserve the records of transactions for an indefinite period. The primary transaction data and metadata can be used for enhanced procedural and financial auditing. Depending on the model of DFC chosen, it might be possible to carry out behavioral analysis, impact analysis of the social security measures.

Broader Implications and Considerations

The Governments may not need to change legal framework to use DFCs. But the role of Central Banks might change significantly after a large-scale roll out of DFCs. The concerns about individual privacy and customer protection, which hitherto were not related to the working of Central Banks,

[6] Tak & Gupta (2019).

would have to be incorporated through appropriate legislative mechanism. Central Bank and Government dynamism would also change and necessitate adaptive decision-making.

A robust DFC ecosystem would need a systemic overhaul. Something that is not accepted for payments is not a currency. If DFC ecosystem is not able to provide robust payment options on account of poor connectivity or legacy systems, it will have negative impact on consumer confidence in DFCs. Customers using Private crypto-currencies understand (or at least supposed to) the risks associated with it. The Governments using DFCs may not have that luxury. So ensuring appropriate infrastructure, foolproof systems, fraud detection and prevention, compensations in case of frauds will be necessary.

Possibility for Further Study: Beyond this report, ITU-T could undertake further study regarding the role of telecommunications agencies in the DFC ecosystem.

6. Financial Inclusion and AML

1. Financial Inclusion

DFC systems are the logical extension of digital payment systems. Governments using DFCs over mobile platforms can significantly reduce the cost of transacting in DFCs making it a viable instrument even for smaller denominations. It can also form the backbone of new credit and savings systems, allowing governments to extend credit, provide savings accounts, and service social security/pension obligations directly via mobile wallets instead of through financial system intermediaries.

Using DFCs as strategy for Financial Inclusion may not as transformational for developed countries, which have near universal financial access; but it can play a significant role in developing and least-developed countries. On the other hand, DFC systems also have the potential to transform cross-border payments which would have significant impacts on international remittances between developed and developing nations.

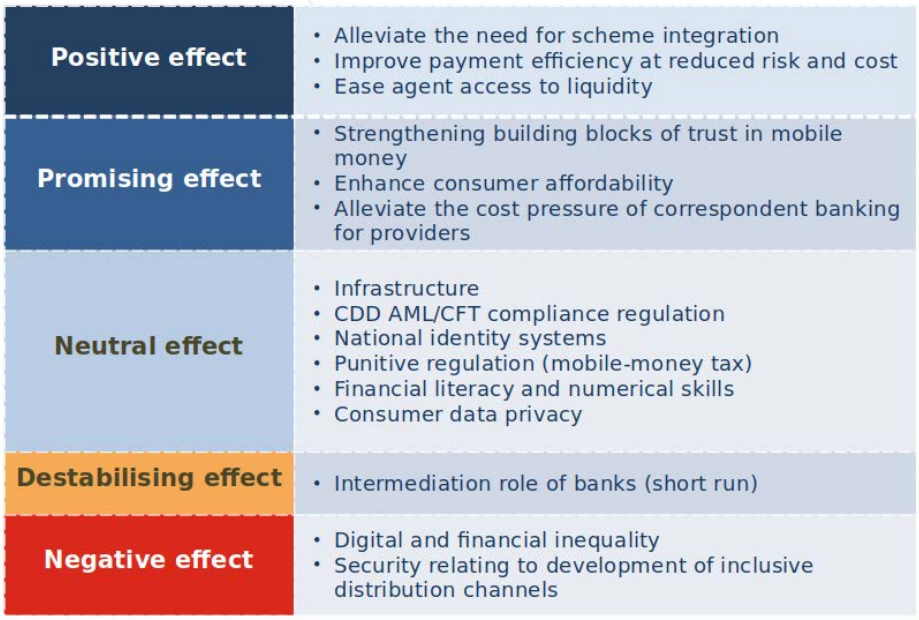
The World Bank estimates that around 2 billion people have no access to any financial services. Overall, only about 59 percent of men and 50 percent of women in developing countries have an account at a regulated financial institution. One of the reasons for the limited access to formal banking is non-availability of brick and mortar banks.

Digitization of payment systems overcomes this problem and has proven to expand financial inclusion worldwide. M-pesa in Kenya, *Aadhar* based Universal Payments Interface in India are examples where technology has expanded financial inclusion substantially.

Despite the importance of digital financial services and its significant impact on financial inclusion, the digital payment ecosystem in many developing countries has lacked the necessary operational and regulatory support framework, such as the use of banking agents and applying a risk-based approach in anti-money laundering and countering financing of terrorism (AML/CFT).

Furthermore, even nations with sophisticated mobile money systems still struggle to ensure universal interoperability between different payments system and wallet providers, despite interoperability being critical to universal adoption.

Jurisdictions considering implementation of a mobile money-linked DFC system for the primary purpose of financial inclusion should consider the broader potential impacts on the financial system, both positive and negative, as outlined for example in the following table:[7]



Possibility for Further Study: Beyond this report, ITU-T SG3 could study the impact of introducing DFC and its economic impact as a means of using ICT to bridge the financial inclusion gap.

2. Anti-Money Laundering (AML)

Anti-money-laundering refers to a set of procedures, laws and regulations designed to stop the practice of generating income through illegal actions. These regulations overlap with, although are somewhat distinct from, Know-Your-Customer (KYC) regulations.

Though anti-money-laundering laws cover a relatively limited number of transactions and criminal behaviors, their implications are far-reaching. For example, AML regulations require institutions issuing credit or allowing customers to open accounts to complete due-diligence procedures to ensure they are not aiding in money-laundering activities. The onus to perform these procedures is on the institutions, not on the criminals or the government.

Scenarios and examples of AML activities are innumerable, ie illegal data access, hacking data and information, illegal database connectivity, mobile phone access of prohibited or restricted data, cyber bullying etc. are some of the methods of capturing private financial data from personal belongings or organization's belongings.

[7] Cooper & Allen (2019).

3. AML Practices Across the Fintech Ecosystem

Criminals exploit money service businesses (MSB) at all stages of the money-laundering process. The following examples illustrate the general methodology for laundering Illicit funds through digital currencies.

Phase 1: Fiat currency to primary digital currency (bank to basic digital exchange)

A global crime syndicate attempting to cleanse illicit U.S. dollars can enter crypto currency markets in two ways: either through purchase of digital currency from a basic digital exchange via the syndicate's bank account, or by cash or debit card at one of over 1,600 U.S.-based digital currency ATMs. Basic digital exchanges are generally preferred, as bitcoin ATM companies are regulated as money service businesses (MSBs), which requires they maintain anti-money laundering (AML) programs. As a result, most launderers open online accounts with basic digital currency exchanges, such as Coinbase, Gemini, Bitstamp, or Kraken, which accept fiat currency from traditional bank accounts. For additional online privacy, launderers may adopt pseudonyms through encrypted email services (e.g. ProtonMail or Hushmail), set up anonymous e-wallets (e.g. Jaxx, Samourai, or BitLox), and run logless virtual private networks (VPNs) (e.g. Mullvad or Windscribe); all via an encrypted, blockchain-optimized smartphone.

Opening a bank account typically requires detailed personal information for account verification. Launderers may use "straw men," or money laundering intermediaries, with clean records and corroborated employment, with direct deposit, to provide an additional layer of separation. They can also purchase fully verified accounts from willing participants on social media forums such as Reddit. Once verified, the digital exchange account can receive fiat currency deposits through wire transfers, automated clearinghouse (ACH) transfers, or by bank account or credit/debit card number. The funds can then be used to directly purchase stake in a "primary coin," such as bitcoin, Ethereum, or Litecoin. These primary coins can be used as an intermediary between fiat currency and alternate digital currencies, or "alt-coins". Alt-coins can only be purchased on advanced exchanges using primary coins (i.e. not with fiat currency). Many classes of alt-coin exist, each with unique purposes. Among these are centralized and decentralized currencies, lightning fast payment-oriented coins, and privacy coins.

While traditional decentralized blockchain coins, like bitcoin and Ethereum, maintain a detailed transaction audit trail, some alt-coins do not maintain a ledger of this information. These node-to-node (N2N) privacy coins encrypt transaction details so that only transacting parties can see them, using privacy features such as "homomorphic encryption," which allows for the data calculations needed to facilitate a transaction without the need to first decrypt the data; and "proof cryptography," which verifies the transaction without revealing the details.

Phase 2: bitcoin mixing - primary coins (basic exchange) to privacy alt-coins (advanced exchange)

Assume the launderer purchased bitcoin with U.S. dollars on the basic Coinbase exchange. The resulting bitcoin ownership would be represented in a bitcoin digital wallet, which has its own unique and traceable digital address, as well as a unique QR code.

In order to obfuscate the primary coin's audit trail, launderers use a tactic known as "mixing" or "tumbling". Mixing services, such as Bitmixer or Helix, perform primary coin address swaps against temporary digital wallet addresses in an attempt to fool the blockchain and break audit traceability. Some advanced exchanges, like ShapeShift, which require no login or verification, may be used as an alternative mixing method. ShapeShift, which operates only through sending and receiving wallet addresses, allows a backup address to be used in the event a transaction fails. Launderers intentionally use false receiving addresses in order to re-route transactions to the backup address, thereby breaking the audit ledger.

The next step is to transfer the mixed bitcoin holdings to an advanced digital exchange, such as Bittrex or Binance, for acquiring privacy coins. The transfer process between exchanges can take hours with bitcoin, while Litecoin and Ethereum generally process in minutes. Once the launderer's bitcoin arrives in the advanced digital exchange bitcoin wallet, they can then trade bitcoin for a privacy coin, such as Zcash, Verge, Monero, Dash, and Desire. Desire uniquely provides its own mixing service within the blockchain itself.

Phase 3: layering through multiple privacy coins, exchanges, and digital addresses

The money laundering layering process involves a series of money movement tactics designed to provide anonymity to the illicit source of funds. Upon purchasing privacy coins on an advanced exchange, money launderers can easily and anonymously layer funds between various digital currency exchanges, privacy coins, and crypto wallets that can belong to anyone. After several layers, money launderers can sever the audit trail, effectively cleansing illicit funds for integration back into the traditional financial system. Having severed the audit trail in Phases 1 through 3, the launderer now has several options for withdrawing the cleansed funds from the digital currency world.

Phase 4: "bust-out" integration

Privacy coin holdings can be re-exchanged for primary coins, which can then be transferred back to a basic currency exchange, where funds may be withdrawn to a connected bank account. If the launderer deems reintegration into retail bank accounts too risky, they can transition funds into real estate, citing the legal, expected desire to avoid capital gains taxes. However, the most secure way to transition funds for integration is to transfer digital holdings to a portable hardware crypto wallet. These flash drive-sized devices provide couriers with the means to avoid risky bulk cash smuggling by transporting funds covertly. In fact, a courier can accomplish the same task with a printout of the digital address or QR code. Laundering cells may further limit access to funds throughout their logistical network by requiring an elaborate passphrase known only to the sender and desired recipient.

4. AML Regulation as ICT Design

Given such risks, counter – AML regulations are an the integral part of digital currency applications. Addressing these needs requires consideration at the ICT-level, as well as the financial regulatory level. This is because fintech applications are built on the design and development of ICT platforms. In addition, it is important to consider regulation of business analytics to ensure there is sufficient commitment to fraud detection and fraud resolution products and services.

7. Unintended Consequences and Possible Risks

1. Central Banking

Existing monetary policy frameworks mainly use interest rate as main policy instrument, where policy interest rate is expected to affect the movement of interbank money market rate, which in turn, is transmitted to the interest rates of bank deposits. The deposit rates mainly serve as interest cost of funds for banks in setting lending rate and as reference for household decisions, whether to consume or save.

The existence of DFC (general purpose), which serves as payment instrument and store of value, may weaken the interest rate elasticity of deposits supply, if households and firms prefer DFC to demand and savings deposits. This is because if a significant amount of bank deposits move into DFC, a large part of broad money will be replaced by base money. At the same time, it would strengthen the central bank's ability to conduct monetary policy through other channels, such as paying interest directly to consumers and retail DFC account-holders.

Alternatively, if the demand for DFC increases, while holdings of physical currency do not significantly decrease, central bank's liabilities will enlarge. Thus, under a DFC regime, central banks may be required to adopt a permanently larger balance sheet, as well as tolerate greater bank reliance on discount window-like direct liquidity provisioning.

Furthermore, if central banks are mandated to lend to commercial banks beyond merely for monetary operation and LOLR purposes, they may need to compromise their asset quality, i.e. by holding a less-liquid and riskier securities, if high quality securities available in financial market are limited. Large buying of securities by central bank may impact market functioning, influencing securities' prices and yields.

Consequently, the central bank's statutory mandate may need to be amended to allow for more targeted credit allocation to the real (non-financial) sectors of the economy, either through direct loan extension or through guiding bank activity. Thus, the core issue may not be about how DFC will affect the existing monetary policy framework, but how a DFC system allows for greater innovation and change from the existing monetary policy framework and operation.

At the same time, any structural or radical changes to the banking system, the role of the central bank in the financial system, and/or monetary policy frameworks and operations may pose risks to financial system stability in the short run, even while beneficial in the longer run. Such changes could be quite risky for a small-open emerging economy in particular. Accordingly, such reforms may require a new coordinated international financial arrangement as a prerequisite in order to be successful.

2. Bank Lending

The introduction of DFC for general purpose poses risks to bank's funding structure and cost, if households' and firms' demand for the DFC is high, but acquired with their bank account money rather than substituting their cash holdings. The extent of this risks depends on the design of such a DFC system, whether it is account- or token-based and interest or non-interest rate bearing. It is also dependent of the cap applied for both account- and token-based DFC. For token-based DFC, the risks might be dependent on whether the transaction is unregistered or registered in central bank. In addition, the more extensive the DFC can play its role as retail payment instrument, the more likely households and firms holds DFC instead of savings deposit accounts in commercial banks.

Banks can respond to the decreased households' and firms' deposit in several ways. First, banks may need to raise deposit rate, thus resulting in a higher lending rate as well. Second, banks can adjust their loan position in accordance with decreased fund. Both responds could lead to economic slowdown.

When banks experience significant deposit outflow, particularly from demand and savings deposit account, they may be forced to fund more of its lending with long term securities and equities, requiring sufficient securities in a liquid domestic financial market or supported by strong capital.

In effect, banking system may need to be changed from the existing "fractional-reserve banking" to “full-reserve banking or "narrow-banking".

Shifting to a DFC-centric banking industry may lead to a more resilient financial system, as such banks can significantly reduce risks of having maturity mismatch, bank run, demand for deposit insurance, and activation of CB’s lender of last resort (LOLR) function. However, the process of this fundamental and radical change may pose risks to financial stability, e.g. adverse development in domestic financial market, particularly for emerging market economies.

It is important to ensure that any transition to a DFC system does not produce an unintended slow down in economic growth by impairing banking lending through increased lending rates. Hence, such fundamental changes, if required, should be coordinated internationally across countries. In addition, regulators must consider the potential and limitations of purely ‘narrow banking’-based business models, particularly in jurisdictions with shallow financial markets and limited access to capital.

3. Legal

Implementation of a new DFC system will raise new legal questions, and require reconsideration of existing legal doctrines that were formulated in light of older technologies and systems. For example, given recent regulatory confusion around the classification of different kinds of private cryptocurrency and blockchain-based assets, it is critical to develop a clear, rational legal classification scheme for the various financial instruments and derivative contract-based products that will emerge from a DFC system.

In addition, central banks must exercise care to ensure new DFC systems are compliant with their legal mandates regarding issuance and regulation of fiat currency and/or legal tender. Further regulatory updates may be necessary in the following areas: issuance of electronic money and systems, service providers, mobile payment accounts, means of identification (certification), passwords, money transfers, interoperability, confidentiality and integrity of information, securing applications, security infrastructure and follow-up, security system assessment, and procedures for obtaining a service license.

DFC systems must also be designed in order to be compliant with civil liberties, privacy and data-gathering laws, and must adopt security and data-protection standards consistent with industry and legal standards. Regulators and DFC operates must also develop a framework for coordination with law enforcement to prevent, monitor, and pursue digital financial fraud, as well coordinate with legal authorities in other jurisdictions to ensure comprehensive enforceability of basic standards and behavior. Furthermore, law enforcement agencies and regulators must ensure sufficient resources are devoted to understanding and addressing new risks associated with DFC technology and the financial activity that will emerge from it.

One possible way of exploring such legal issues experimentally is through the creation of a regulatory ‘sandbox’ in which different products and systems are tested and evaluated. However, such initiatives must be careful not to weaken overall regulatory enforcement efforts and/or become a vehicle for regulatory manipulation by industry interests.

4. Technical

Greater adoption of DFC at the expense of physical cash and coins increases vulnerability to digital and/or electric system failure. In addition, networked forms of digital currency that require validation by a centralized authority, or in which data is maintained in a centralized repository, increase the risk of single-point-of-failure vulnerabilities and/or security breaches. Addressing such risks requires

significant resources and state-of-the-art technology and human capacity. Such capacity may not exist in smaller countries, or may be unsufficient to protect them against better-resourced competitors.

Alternatively, nations with unstable or dysfunctional government may struggle to achieve necessary political consensus on core regulatory and design issues necessary for implementation of DFC, resulting in inertia and/or loss of support for further investment. Such issues include, for example, establishing common standards for interoperability between private networks, and establishing necessary dispute resolution and regulatory systems to ensure smooth and legal market functioning. Addressing such issues may require aggressive early planning and intervention, establishment of peak-body stakeholder organizations and legal infrastructure, a statutory commitment to open, common standards-development, and adoption of best practices standards from adjacent industries and regulatory bodies.

5. Implementation

Introducing a DFC system without the necessary prerequisite infrastructure, engineering expertise, regulatory and policymaking support, and/or industrial capacity increases the risk of financial harm and even systemic crisis.[8] Mitigating such risks requires adequate investment in domestic capacity-building, as well as external experts to train local stakeholders, prioritize simplicity and usability as core design features.

Budget mismanagement and/or poor roll-out could undermine public and political support for DFC, causing the program to be underfunded, poorly managed, and/or ultimately terminated. Alternatively, insufficient attention to stakeholder concerns and opposition criticisms could generate political pressure to reduce scope or terminate program, regardless of positive outcomes. Mitigating these risks may require an explicit diplomatic strategy for generating, monitoring, and retaining political and stakeholder support for project during planning and implementation phases, as well as transparent budgeting and decision-making, with regular external audits.

In addition, it is possible that the resource, implementation, and regulatory compliance costs of DFC outweigh the immediate economic benefits to users and firms, increasing public resentment and industry opposition. Such risks could be mitigated by minimizing regulatory pass-through costs and focus on consumer, business, and intermediary adoption and ease-of-use as top implementation priorities.

[8] For more information on potential risks and unintended consequences related to mobile money specifically, see Cooper & Allen (2019).

8. Conclusion

DFC provides an alternative vision of the future of financial services than a world of private cryptocurrencies. At the same time, it provides opportunities for governments to attain their financial inclusion goals, while cutting payments system costs and improving delivery of public services and public budgeting.

While DFC has the potential to significantly improve public policymaking, there are still some areas that require further research. In particular, security issues must be researched further to ensure that any widely adopted DFC system would be sufficiently protected against fraud and cyber-attacks. Another area for further study is the legal and regulatory framework underpinning the DFC ecosystem. Some legal questions merely require adopting standards and practices from adjacent areas. Others will require original thinking.

Finally, further research is needed to identify the full range of stakeholders in the DFC ecosystem, and to ensure they are involved in future discussions. This includes not only government and financial institutions, but also telecommunications actors, privacy experts, and members of community groups and the public.