CBDC PAPER

DESIGN AND APPROACH

JUNE 2022

FARI SOLUTIONS

AUTHOR | SHAFIQ AMIRI

CONTENTS

ABBREVIATIONS

CBDC	Central Bank Digital Currency
RTGS	Real-Time Gross Settlement
DeFi	Decentralized Finance
AML	Anti-Money Laundering
CFT	Combating the Financing of Terrorism
DLT	Distributed Ledger Technology
GDP	Gross domestic product
KYC	Know Your Customer
BIS	Bank of International Settlements
P2P	Peer-to-Peer / Person-to-Person
DvP	Delivery-versus-Payment
Pvp	Payment-versus-Payment

PREFACE

Once dominated solely by banks, the recent decade has seen the finance industry entering a dynamic environment of fast changing standards and products. Traditional banks have long served as an intermediary for the end-user to access money, but with rapid technological advances and innovation stemming from the private sector, the financial industry's landscape has begun to shift. The rise of digital assets such as Bitcoin, have served everyone a new question: what is cash?

Elements of the private sector have rushed to explore areas where digital assets can be integrated into existing systems or even to adopt a new one. This has undoubtedly created competition within the industry and is now forcing participating entities to innovate or risk being left behind. Another question that arises within this quick-paced phenomenon is what is now expected of central banks, and what role can they play?

Salt and metals which were once used as currencies and a medium of exchange, transformed into fiat cash for universal adoption. Presently, the way society perceives payments coupled with the need for comfort and ease, brought the wide usage of credit, cheques, and card payments. Just as card payments made cheques redundant, now rises a new form of value exchange - digital assets.

The Covid-19 pandemic has increased the need for a more distant payment structure to better facilitate health guidelines and to fulfil broader consumer demand. But as we combat the pandemic, will the changes that came into effect eventually revert back to what it once was?

In recent years, digital assets have exploded onto the financial scene, and while they are not yet mainstream, digital assets do appear to be getting adopted, both by consumers and businesses offering novel types of investment products and payment methods. The start of the cryptocurrency, Bitcoin, offered an alternative lens as to how we view the distribution of value and information. Since 2009, people have strived to better Bitcoin, and in doing so, initiated the creation of other decentralized digital currencies. Whether by design or by accident, these digital assets brought forth decentralized finance (DeFi). DeFi and cryptocurrencies have been subjected to a fair share of both criticism and praise, with the ability to enhance financial inclusivity taking the limelight at a time where 1.7 billion people are unbanked, globally[i].

Central Banks (being the apex regulator of the financial markets) and their respective national currencies, have rushed to study the rise and potential risks of decentralized currencies and decentralized finance. Today, central banks are pressed to deal with these private cryptocurrencies as they pose a threat to core objectives of a central bank i.e. maintaining the purchasing power of their country's currency, and managing risks tied to financial stability.

Per Andrew Bailey (Governor of the Bank of England), Bitcoin and decentralized currencies pose a global financial stability risk in the near future[ii]. However, as consumers start to use cryptocurrencies, the central banks must probe this medium. One way to contain the rise of private digital currencies is to issue a regulated central bank digital currency (CBDC). Hoping to dissuade the population from partaking in a volatile market, a CBDC must strive to extract the benefits of cryptocurrencies, add to efforts which mitigate risk of financial stability and fulfil consumer needs. Today, central banks representing 90% of the world's GDP, are in some form of engagement with CBDC, the majority of which are researching the topic, while a few have already launched or are doing pilot tests[iii].

To curtail currency substitution risks, central banks will have to take the next step, but is introducing a basic CBDC the answer, or should there be a nuanced technical CBDC structure that not only supports all stakeholders, but gives them a platform to flourish.

[i] https://globalfindex.worldbank.org/sites/globalfindex/files/chapters/2017%20Findex%20full%20repor
[ii] https://www.reuters.com/world/uk/boes-bailey-tells-banks-be-careful-with-crypto-2021-12-13/
[iii] https://www.atlanticcouncil.org/cbdctracker/

1.0

CENTRAL BANK OBJECTIVES

Recent interest sparked by rising private digital currencies has truly pushed for deeper understanding into the need for a CBDC. As countries around the globe research, experiment or implement a CBDC, the outcome can serve as a benchmark or a lesson for observing and early-stage central bank digital currency projects.

While central bank views differ, the majority are inclined to test a retail CBDC, with a recent accelerated effort in advanced economies due to Covid-19 and cryptocurrencies.[iv]

The intended objectives of introducing a CBDC at a foundational level can translate to:

- Maintaining financial stability
- Containing the risk of currency substitutions
- Improving domestic and cross-border payment efficiencies
- Providing wider access of financial products to the population
- Fostering innovation in the payment sector

[iv] Bank for International Settlements: Paper 125

Central banks will choose to test and prioritize different forms of CBDC based on their objectives and any technological limitations that may arise. The two main types of CBDC that have taken centerstage are retail – which is aimed primarily for person-to-person payment facilitation – and wholesale CBDC that is aimed at handling large-scale payments.

2.0 DESIGN

2.1 ACCESSIBILITY

The level of access attributed to any CBDC would largely depend on the exact objectives that have been outlined by central banks which influence the form of CBDC to be created. Much like the real-time gross settlement (RTGS) system which is open only to financial institutions, a wholesale CBDC would be alike in accessibility design. On the other hand, a retail CBDC designed to improve financial inclusion, and domestic end-user payments would be open for all to use. This degree of open access can be achieved with tiered know your customer (KYC) checks.

Traditional KYC checks however, involve a person having to visit a bank's branch, which is part of the looped issue of fragmented banking access due to geographical and fiscal limitations. One of the contributing factors of low financial inclusion is the absence of banking facilities within remote locations where opening a branch is not feasible for a bank. To solve this issue, retail CBDC access can be limited to the extent of KYC information furnished by an end-user. Digital identity and other novel solutions can play a part in streamlining the on boarding procedure.

Whilst the aforementioned points highlight potential technical barriers, central banks and stakeholders have to take end-user receptivity into consideration as well. educational campaigns

have to be initiated to establish trust whilst promotional campaigns can be utilised to expand usage of the CBDC throughout the population. This section of a CBDC can be tackled by public-private engagement.

Lastly, the access gateway of a CBDC falls under the following two categories:

1 Tier

CBDC is issued and distributed by a central bank, and end-users directly interact with the central bank itself. The end-user would be able to redeem their CBDC for cash with the central bank.

2 Tier

CBDC is issued by a central bank to intermediaries (banks, payment service providers, etc.) and intermediaries would open an account for end-users and distribute the said CBDC. The end-user would interact only with the intermediary, and the intermediary interacting with the central bank, effectively creating two tiers of communication.

In either model, the accounting ledger could be set up in a manner where a central bank can view transactions by end-users individually, or as an aggregate of transactions through intermediary ledgers. However, all main functions of issuance and redemptions are reserved by the central bank.

2.2 DOMESTIC AND CROSS-BORDER PAYMENTS

Much of the deliberation taking place on the introduction of a CBDC relies upon the main function of the digital currency; specifically, whether the proposed CBDC is to serve the domestic population or become a tool to improve cross-border payments.

Cross-border payment functionality has been prioritized by advanced economies which mostly employ robust instant payment systems, and who may not currently consider a retail CBDC a necessity. Emerging markets and developing economies however, would see a retail CBDC as a means of extending financial inclusion and promoting innovation.

Around the clock CBDC enabled cross-border payment is a use case that is being studied; however, interoperability is needed to achieve efficiency in this field. Given the differing

technology providers and infrastructure being used to test and deploy CBDC globally, harmonization of these systems is needed in order to communicate and make international payments.

The Reserve Bank of Australia, Central Bank of Malaysia, Monetary Authority of Singapore and South African Reserve Bank have all been testing the so called "multi-CBDC" or mCBDC in partnership with the Bank for International Settlements to test international payments [iv]. But as the CBDC journey is still within the early stages of development, it's still unknown what innovative solutions could potentially address this issue.

2.3 OPPORTUNITIES

The introduction of a digital currency has the potential to open gateways of different opportunities and benefits to all stakeholders. Select preconditions like cost efficiency, levels of anonymity, programmability and others can transform a CBDC into a platform that enables heightened participation from end-users and the private sector.

Current CBDC types and use cases include:

Retail CBDC
To facilitate peer-to-peer, instant payments, where consumers can pay for goods, services and one another with "digital cash" backed by the central bank.

Wholesale CBDC
Serve as a settlement and reconciliation channel for high value payment systems and digital financial markets.

Cross-border payments
Instant cross-border payments, can be designed for use by both "Retail" CBDC and "Wholesale" CBDC.

Special purpose CBDC
With the programmability of blockchain smart contracts, special purpose tokens can be issued that can only be used under certain conditions or areas, e.g. social aid payments.

[v] https://www.bis.org/about/bisih/topics/cbdc/dunbar.htm

CBDC can optimize cash circulation, including lowering the costs associated with transportation, security, etc. The application of a CBDC has the potential to make way for an innovative set of prospects within the payments sector, benefiting all stakeholders alike.

These inherent preconditions and technical capabilities can pave way for the:

State

- Foster competition, and development of the financial sector
- Efficient and transparent social and government payments
- Improve implementation of monetary policy

Businesses

- ·Provide new services by utilizing programmability of a CBDC
- ·Optimized auditability using Distributed Ledger Technology (DLT)
- ·Lower transaction fees and cash handling costs

End-users

- Payment system accessibility in remote areas with lack of infrastructure
- Lower fees for remittance and payments
- Improved payment security

Financial institutions

- ·Lower cost of cross-border payments
- ·New revenue stream by introducing innovative services
- ·Instant and direct settlement

2.4 DISTRIBUTED LEDGER TECHNOLOGY (DLT)

DLT or blockchain is the technology behind the decentralized digital assets; Bitcoin, Ethereum, etc. and DLT is the main technology that's being tested for CBDC due to the programmable nature of the blockchain which allows for writing and executing smart contracts. However, public and decentralized infrastructure is not a realistic option for central banks which requires operations in a regulated environment.

Central banks are opting for private "permissioned" DLT where participation and access to the CBDC platform is authorized by the regulatory body, and because private DLT can handle higher transaction volumes. The underlying technology which will power any future CBDC platform must also be able to facilitate an estimated growing demand of such a CBDC. The ability to support the required transaction volume would play a key role in the central banks' decision when selecting the technology.

The Bitcoin network handles an average of 5 transactions per second – a performance that is not sustainable for a fully operational retail CBDC where transaction volume could exceed thousands per second.

Whether retail or wholesale CBDC is selected by a central bank, certain technical abilities are necessary for a functional CBDC whilst also maintaining security of the infrastructure.

The technology must cater to providing the functions for:

- ·P2P (Person-to-person/peer-to-peer) transactions.
- ·Programmable money
- ·Permissioned access
- ·Decentralized custody of funds.
- ·Improved security by cutting off single point of failure

The technology must also be capable of blocking double spending; an action where the same asset has been used multiple times. Furthermore, the technology of a CBDC platform should also complement existing infrastructure and payment systems.

2.5 PROGRAMMABILITY

Perhaps the most significant area of a CBDC will be the programmable nature of digital cash and how it will influence the future of transactions. While “programmable” transactions have existed in some form before, the level of control and automation brought by DLT smart contracts ensures that outcomes are always dependent on programmed conditions.

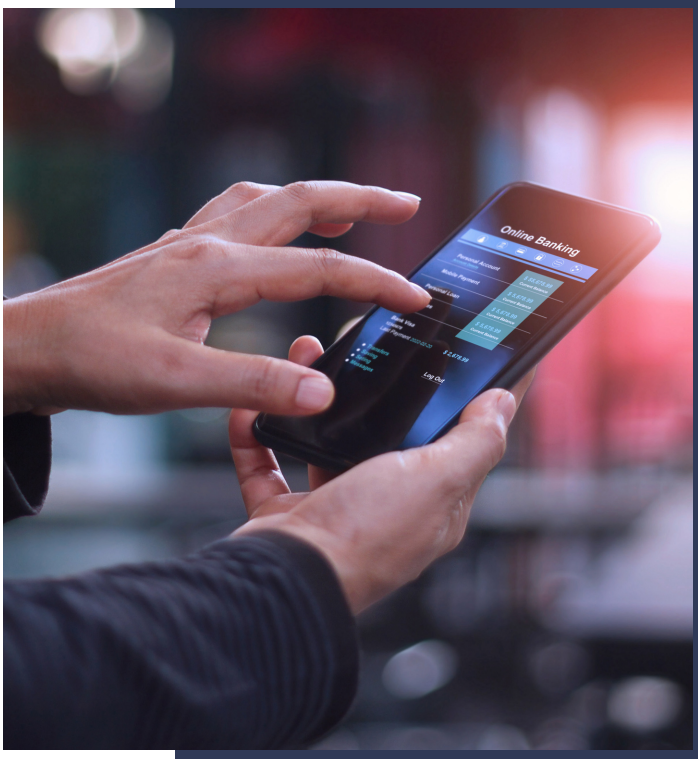
Programmability can be embedded within multiple areas of a CBDC, ranging from governance and transactions, to limitation of participants and access.

A deeper look into the aforementioned areas can be:

- Different level of access for market players, including their functions, e.g. end-user onboarding or addition of other participants.

- Transaction programmability that controls expenditure based on geography, tier of KYC check, or conditions of “helicopter” money which can be limited to certain merchants and even products.

- Programmability for innovation that allows for built fintech applications to fulfill atomic settlements and provide DvP mechanisms for securities settlement.



3.0 SECURITY

3.1 USER PRIVACY

Regulators are keen to preserve as much of cash-like properties for a retail CBDC as possible, including features such as wide acceptance, anonymity and instant settlement. Nationwide acceptance is achievable as a CBDC would be redeemable one-to-one of fiat cash and will serve as legal tender (assuming the population has a high general knowledge of the matter). Technical features of the underlying technology relating to transaction finality would furthermore ensure CBDC transactions are settled instantly.

Anonymity becomes an issue in a digital atmosphere, where the CBDC design must ensure there won't be regulator overreach whilst allowing the central bank to enforce AML/CFT policies. Controlled transparency of the end-user is being explored to provide remedy in this arena.

In an intermediary-based CBDC design, user privacy would work in a similar manner to current consumer banking laws, with an option of controlled access to a CBDC via tiered KYC procedure. User privacy can be preserved depending on level of KYC information provided and will remain the obligation of the intermediary to secure the given data. On a basic level, transactions can remain anonymous provided that the transaction does not exceed parameters set to be compliant with AML/CFT guidelines.

Anonymity and user privacy are distinct from one another. Anonymity being complete anonymous transactions and participation in the CBDC platform, and the latter safeguarding the end-users' actions and personal data under normal conditions.

3.2 ZERO-KNOWLEDGE PROOF

An additional method of ensuring user privacy is the use of zero-knowledge proof protocols. Given the amount of data generated by a potential CBDC (whether it be personally identifiable data, transaction data or any other type of data), it is imperative that it's handled securely and with utmost care.

Potential issues that may arise include internal mismanagement, or external attacks. While the generated data would be valuable in different use cases of business or economic policy, the regulator may want to have special purpose access to this data for AML/CFT purposes.

To ensure the CBDC data sets are fault-proof, the central bank can seek to deploy different solutions. One such solution would be to rely on cryptography through programming zero-knowledge proof protocol, where data is verified to be true, but the data itself is not shown. Other solutions may be employing a third-party as data managers.

3.3 OPERATIONAL RESILIENCE

The nationwide acceptance of a CBDC also means offline payments.

Perhaps the most common cash-like property that is sought after is for the CBDC platform to be capable of performing secure transactions while offline. The need for offline payments is crucial to central banks who are pursuing financial inclusion as part of introducing a CBDC. Remote areas where there is a lack of connectivity or access to finance due to absence of banks needs a CBDC that can remain operational within these conditions. Furthermore, countries which are prone to natural disasters and who may experience electricity and connectivity downtime would have more emphasis on offline capability.

Whilst offline payments may be possible, a CBDC that synchronizes and validates transactions in real-time might face double spending occurrences in the absence of the internet. As such, practical and secure design of the CBDC platform is necessary to ensure resilience.

Assuming a CBDC will integrate within the national or international payment landscape, the system must also ensure scalability beyond the number of transactions tested during a pilot stage. The underlying technology must be robust enough to avoid being overwhelmed at a point of heightened transactional activity.

The system should ensure high throughput, rapid transaction finality and be able to process equal to or exceed the performance of existing payment processing networks.

3.4 QUANTUM COMPUTERS

Emerging technologies like quantum computers will be capable of breaking data encryptions algorithms used today in many critical infrastructures. Whether a DLT is employed to power the CBDC infrastructure or not, elliptic curve digital signature algorithm (ECDSA) is widely used for data encryption.

The majority of existing blockchains like Ethereum use elliptic curve cryptography to sign transactions, which would be compromised by future quantum computers [vi].

Regardless of the advancement of quantum computers, central banks would need to adopt proactive measures and implement quantum-resistant cryptography to protect data related to the user and transactions, as well as user funds.

[vi] https://www2.deloitte.com/nl/nl/pages/risk/articles/quantum-risk-to-the-ethereum-blockchain.html

4.0 APPROACH

4.1 GOVERNANCE

CBDC being a new concept, has not yet been adopted on a global scale. the international experience, specifically on the regulatory side, is therefore minimal. A comprehensive regulatory mechanism with legal certainty needs to be created to address potential issues that may arise from the complete implementation of CBDC in the economic and financial apparatus.

Risks pertaining to the following must therefore be monitored:

- Financial stability
- Monetary policy
- Financial institutions

To avoid unforeseen circumstances, a strong economic model has to be created to test the outcome of CBDC issuance and circulation. The model should dive into the role of the participants, as well as outlining whose balance sheet the CBDC will be recorded on as a liability or an asset. A study into this should also highlight whether issuing CBDC will have any effect on money supply and potentially raise liquidity issues in case of outflow of funds.

Fully employing the programmability of the technology infrastructure on a network level will set concrete governance guidelines that will differentiate between participants, their respective roles and provide the framework of end-user transaction and identifying data. Further parameters can be introduced by leveraging cryptography and setting user and CBDC supply limits.

4.2 ROLE OF THE PRIVATE SECTOR

The regulator may deem the “one tier” design necessary if traditional financial institutions have not been able to penetrate their respective local banking market, and financial inclusion remains at a lower level. In this scenario, the private sector would have a minimal role in the CBDC ecosystem whilst the central bank would provide direct end-user service. Emerging markets and developing economies may gravitate more towards this approach.

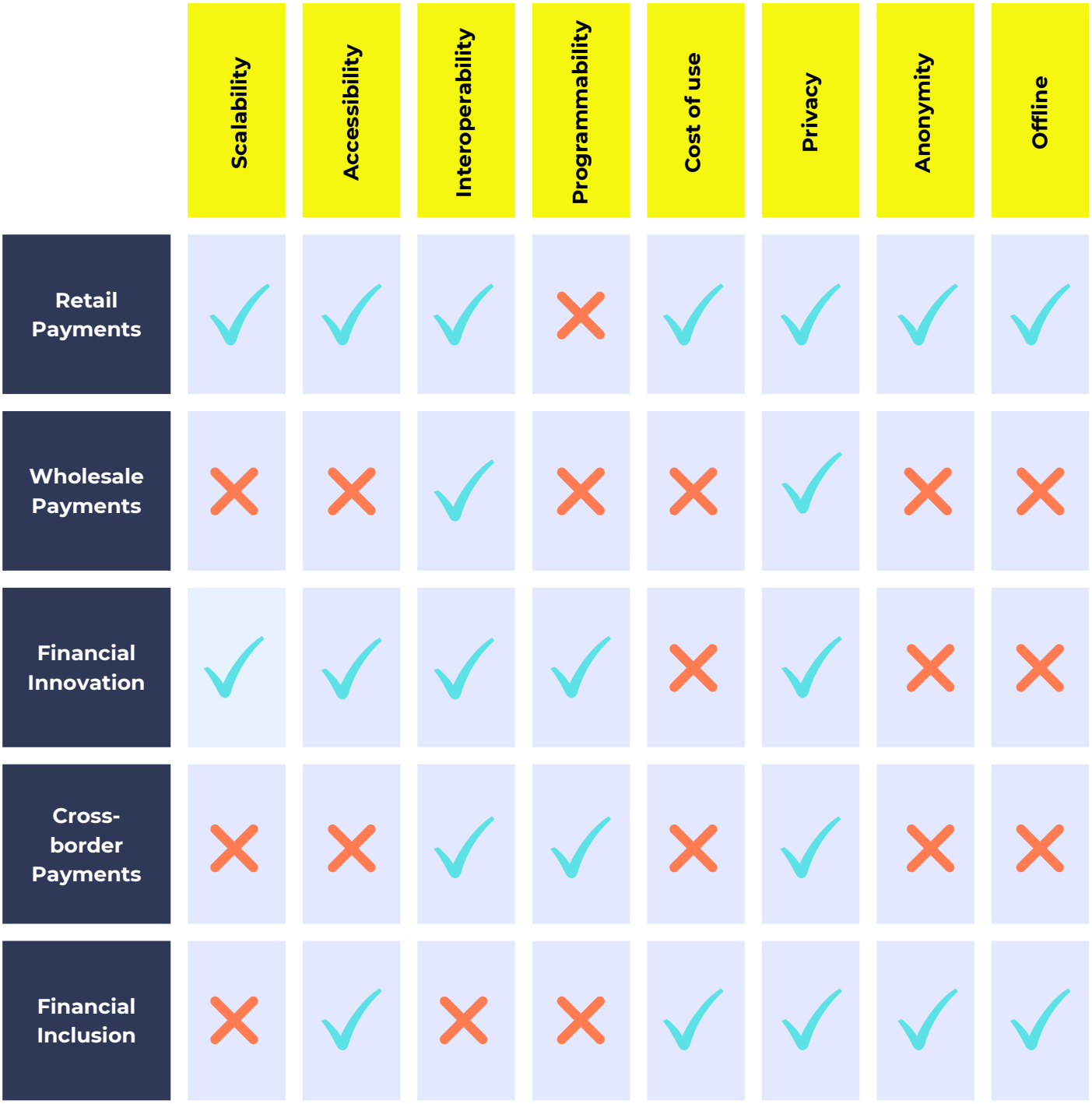
The more prevalent choice of CBDC design features “two tier” access, where the CBDC is issued by the central bank, and the responsibility of distribution and on-boarding is given to intermediaries, such as banks. By design and network layer programmability of the CBDC, the central bank will be able to appoint specific roles to participants and control access to the platform. The private sector would remain intermediaries within this design choice and extend existing services to end-users.

Based on design and capability of the underlying DLT, the CBDC platform can further include programmability for applications built on top of the CBDC. This technical and design feature enables an additional possibility of private sector engagement and encourages innovation in the payments and fintech market.

4.3 FARI DECISION MATRIX

Central banks can refer to the following Decision Matrix to assist in deciding features in relation to their core objectives of introducing a CBDC. Anonymity is applied on a controlled level to allow the CBDC to mimic the anonymous nature of paper cash payments.

Programmability of a CBDC may not be a priority if the sole objective of a central bank is to promote financial inclusion. However, if the policy dictates innovation within the payments industry, then the programmable feature of a CBDC must take precedence in pursuit of encouraging market participants to unlock the full potential of a CBDC through the use of smart contracts.



4.4 CONCLUSION

The response to decentralized currencies, digital assets or cryptocurrencies seems to be a central bank digital currency, coupled with heightened interest tied to the disruption caused by Covid-19 pandemic, and changes in finance and technology. Serving as a legal tender, CBDC is a regulated digital currency issued by the central bank, which is one and the same with the national fiat currency. This is to be either used to pay for shopping, services or one another (retail CBDC), or as a means of settlement between financial institutions (wholesale CBDC).

According to the Bank of International Settlements (BIS) survey, 86% of global central banks are actively studying CBDC and 14% have already engaged in CBDC pilot projects [vii]. Some of the most advanced pilot projects being:

Bank of Sweden:
First in Europe to start piloting CBDC

People's Bank of China:
Most advanced CBDC project, also conducting cross-border payment pilot

The need for anonymity and preservation of cash-like properties stands. While central banks may not want complete anonymity (due to AML/CFT processes), nor zero anonymity (to uphold consumer privacy concerns), a hybrid model has to be taken into consideration. A controlled level of anonymity needs to be introduced to ensure AML/CFT initiatives are being utilized.

Regardless of the international interest in CBDC, there are certain barriers to overcome when implementing such a platform. While some countries have taken the initiative to pilot or even launch a CBDC, the majority are still looking and studying other central banks' moves. The main barriers to international adoption of a CBDC is:

Technology
Distributed ledger technology (DLT) is deemed the popular choice for basing a CBDC on, however, one can not detract from the novelty of the technology. DLT is considered new and lacks experience from developers and users. To move forward, the technology must see keen interest from regulators.

Legacy system
Inability to interop with legacy systems will result in a barrier that might render CBDC unfeasible despite growing trends in cashless payments.

Disruption
Developing a CBDC platform would require coordination with subject matter experts, market participants and stakeholders to best facilitate their needs. Banks' longstanding role as intermediaries will come under threat if certain CBDC designs are followed, e.g., direct CBDC distribution by a central bank.

Barriers to a CBDC are not just technical, but also economic. Engagement with stakeholders is the optimal route of understanding the needs of the market and consumers.

[vii] https://www.bis.org/publ/bppdf/bispap114.pdf

The growing popularity of digital assets and stable tokens is making the argument that a central bank digital currency is in need, however central bank's approach towards implementing a CBDC should be nuanced, taking a multitude of factors into consideration. A significant objective of central banks around the world is the growth of financial inclusion within their population, and a CBDC would be tested to prove efficiency. Some countries who are struggling with unsatisfactory financial inclusion rates despite having digital payment systems, see CBDC as the answer.

A more urgent necessity of a retail CBDC would be the ease of payment as well as serving as a deterrent to digital assets and currency substitution risks. The digital asset market is an unregulated and highly volatile environment, which has resulted in billions of dollars in losses and fraud. The recent de-peg of Terra/Luna algorithmic stable token has caused a loss of $40 billion in value alone. Programmability of a retail CBDC could function as the infrastructure of a fully regulated platform to build financial products and may even dissuade users from the high risks associated with DeFi products.

A wholesale CBDC relates to streamlined cross-border payments that would potentially reduce transaction times and fees, whilst also increasing working hours to a 24/7 format due to automation afforded by smart contracts.

It is therefore recommended to further explore CBDC use cases in addition to the benefits and risks to economic agents. Regulatory questions should be answered in relation to the overall design and consumer protection, as well as engaging stakeholders to observe possible disruptions and address market concerns. A test has to be conducted which contrasts the existing payment systems and CBDC. A comparative analysis must be undertaken with the result of such test concluding whether the existing payment systems can solely fulfil central bank objectives, or if CBDC serves as a better choice. It is entirely possible that a potential CBDC can coexist, or even integrate with the existing digital payment mechanism to minimize the need for new training, development and public awareness modules that would otherwise be required from the introduction of a standalone CBDC. However, features such as settlement finality, P2P transfers, controlled anonymity (that address AML/CFT requirements) and others are core to a robust central bank digital currency platform.

A robust and resilient CBDC platform should take future security issues related to quantum computing into consideration as advancement in technologies would create opportunities and risks. Elliptic curve cryptography which is in use by virtually all blockchains can be compromised [viii]. The CBDC platform must also ensure operational performance by having a scalable infrastructure capable of handling large volume of transactions at any given time. Other costs related to training of technical resources can be saved by utilizing DLT that supports popular and reliable programming language within the virtual machine.

[viii] https://www2.deloitte.com/nl/nl/pages/risk/articles/quantum-risk-to-the-ethereum-blockchain.html