Summary of WP Student Team

Innovation, Digital Business and Technology Strategy

Group constitution:

Student Name	Program	Individual Title
Michelle Bader (50818)	Management	Challenges of CBDCs Privacy - how to Safeguard Consumer Privacy Without Facilitating Illicit Financial Activity?

Work project carried out under the supervision of:

Advisor: João Castro

Reading observations for jury:

A Work Project, presented as part of the requirements for the Award of a Master's degree in Management, from the Nova School of Business and Economics.

IMPLICATIONS AND CHALLENGES OF CBDC'S PRIVACY – HOW TO SAFEGUARD CONSUMERS PRIVACY WITHOUT FACILITATING ILLICIT FINANCIAL ACTIVITY

MICHELLE BADER

Work project carried out under the supervision of:

João Castro

16/12/2022

Declaration of Authenticity

I hereby declare that the paper presented is my own work and that I have not called upon the help of a third party. In addition, I affirm that neither I nor anybody else has submitted this paper or parts of it to obtain credits elsewhere before. I have clearly marked and acknowledged all quotations or references that have been taken from the works of others. All secondary literature and other sources are marked and listed in the bibliography. The same applies to all charts, diagrams and illustrations as well as all to all Internet resources. Moreover, I consent to my paper being electronically stored and sent anonymously in order to be checked for plagiarism. I am aware that if this declaration is not made, the paper may not be graded.

Lisbon, 14th December 2022

Location/City, Date

Signature

_____

Michelle Bader (50818)

Abstract

The rapid decrease in the use of cash and the emergence of stable coins and other private digital currencies have led Central Banks to consider the issuance of their own digital currency (Central Bank Digital Currency, so-called CBDCs). This thesis investigated the impact that CBDCs will have on the economic, privacy and technical pillars. To this end, a literature review was conducted in every section, combined with structured expert interviews. The analysis of the economic implications concluded that CBDCs might reduce the need for unconventional monetary policies and that the risks to financial stability are highly dependent on the CBDC design. The analysis of privacy and illicit financial activity concluded that the results ultimately hinge on its technical design and the policy objectives of each jurisdiction. However, the technical frameworks should have the backbone of an efficient legal framework. Since these economic and privacy implications depend highly on the design choices of the r-CBDC, the CBDC needs to be carefully designed without sacrificing user privacy or causing commercial bank disintermediation.

Keywords: *Blockchain, CBDC, Central Bank, Commercial Bank, Cryptocurrencies, Design Choices, Digital Assets, Financial Stability, Illicit Financial Activity, Money, Privacy, Security*

This work used infrastructure and resources funded by Fundação para a Ciência e a Tecnologia (UID/ECO/00124/2013, UID/ECO/00124/2019 and Social Sciences DataLab, Project 22209), POR Lisboa (LISBOA-01-0145-FEDER-007722 and Social Sciences DataLab, Project 22209) and POR Norte (Social Sciences DataLab, Project 22209).

Table of Content

List of Abbreviations

AC	Atlantic Council
AML/CFT	Anti- money laundering and countering the financing of terrorism
BCBS	Basel Committee on Banking Supervision
BCG	Boston Consulting Group
BIS	Bank of International Settlements
CBDC	Central Bank Digital Currency
CFR	Charter of Fundamental Rights of the European Union
DCEP	Digital Currency Electronic Payment
DeFI	Decentralized Finance
DLT	Distributed Ledger Technology
DPoS	Delegated Proof of Stake
EC	European Commission
ECB	European Central Bank
ECtHR	European Court of Human Rights
EP	European Parliament
EU	European Union
EUCO	European Council
FED	Federal Reserve System
GDPR	General Data Protection Regulation
HM	Helicopter Money
IFF	Illicit Financial Flows
IFRS	International Financial Reporting Standards
IMF	International Monetary Fund
KYC	Know your customer
P2P	Peer-to-peer
PBoC	People's Bank of China
PKC	Public Key Cryptography
PoA	Proof of Authority
PoS	Proof of Stake
PoW	Proof of Work
QE	Quantitative Easing

R-CBDC	Retail CBDC
SBA	Swedish Bankers' Association
TRM	The Royal Mint
UTXO	Unspent Transaction Output
W-CBDC	Wholesale CBDC
ZKP	Zero-Knowledge Proof

Group Part

Chapter 1: Introduction

Money and payments are essential components of our society and economy. Digitization and financial technology breakthroughs are rapidly transforming economic life, destabilizing society, and reinventing all aspects of existence. These technological breakthroughs of the twenty-first century have not been immune to financial architecture. Consumer spending habits and the need for quick payment solutions are influencing digital transformation. Cash usage is diminishing, as new types of digital payment choices emerge.

The financial system is witnessing the advent of new asset classes with the arrival of new digital means of payment (such as cryptocurrencies like Bitcoin and stable coins like Tether), but also examining the potential scope for innovation in conventional structures. Meanwhile, there is rising interest in a revolutionary payment ecosystem: Central Bank Digital Currencies (CBDCs). Central Banks and governments are steadily investigating and piloting the architecture of a CBDC. The composition of this digital asset is quite vague, as seen by the multiplicity of proposals suggested by various Central Banks. A CBDC is a prospective new payment system solution that represents a digital version of fiat money that may be accessible globally and possibly have legal tender status, despite the fact that the notion of a CBDC was introduced years ago (Tobin 1987). CBDCs are not cryptocurrencies, such as Bitcoin or Ethereum. The only thing they may have in common is the technological platform they use, namely distributed ledger technology (DLT). CBDCs do not require specific technology, as they can be built on different technologies. However, the emergence of cryptocurrencies has brought their underlying technology into focus. In addition, cryptocurrencies are not issued by Central Banks and can be extremely volatile, as recent movements in the crypto market illustrated (Bakas, Magkonis and Young 2022). CBDC, on the other hand, would constitute a liability to the Central Bank, similar to banknotes. While most people find it difficult to comprehend, the Sand Dollar project in the Bahamas became the world's first launched CBDC

in 2020, and the Chinese currency (e-CYN) has already been tested in numerous pilot projects (Laboure et al. 2021).

Not only are new technical possibilities the main drivers for CBDC, but so is the gradual drop in cash usage. At the same time, crypto assets seek to market themselves as a complementary payment method to existing payment methods. The paper investigates possible challenges and implications of a CBDC via three lenses: financial stability, technological design, and privacy. The goal is to offer an overview of the still rather sparse CBDC literature and draw on expert knowledge. Finally, the paper does not advocate the issuance of a CBDC, as the ultimate decision to issue a CBDC depends on political factors. The paper rather offers recommendations on how to mitigate risks under various circumstances.

1.1 Background and Overview

1.1.1 What is meant by a Central Bank Digital Currency?

There are a variety of definitions for "Central Bank Digital Currency" that have been proposed in the literature, which is due to the diversity of concepts and designs of a CBDC. Among the multitude of existing definitions, there is no universal definition of the concept. Kochergina and Yangirovab (2019, 83) state that a CBDC is "*an electronic obligation of the Central Bank expressed in a national monetary unit and acting as a means of exchange and store of value*". Similarly, Kiff et al. (2020, 9) describe a "*CBDC as a digital representation of a sovereign currency issued by and a liability of a jurisdiction's Central Bank or other monetary authority".*

More recently, several Central Banks, including those of Sweden, the European Union, Japan, the United States, etc., along with the Bank for International Settlements (BIS), have joined forces to coordinate and consolidate their research on CBDCs and produce a report summarizing their common position. In this paper, a CBDC is defined as "*a digital form of Central Bank money that is different from balances in traditional reserve or settlement accounts. A CBDC is a digital payment instrument denominated in the national unit of account*

that is a direct liability of the Central Bank" (BIS 2020, 3). At the most basic level, a CBDC is an electronically stored monetary value established by regulatory authorities (governments, Central Banks) which is a liability to the Central Bank and has the properties to make payments. It is evident from these definitions that a CBDC in the literature is a Central Bank obligation that differs from currency in its physical features, despite the fact that a CBDC fulfills the same purpose as cash, in fact, to make payments.

1.1.2 Motivations, and risks for issuing CBDCs

The section examines motivations that lead Central Banks around the globe to consider issuing a CBDC but also outlines risks that are associated with the issuance of a CBDC. There are several motivations for the issuance of a CBDC: financial inclusion, financial stability, payment efficiency, payment security etc., which are discussed below, among others.

In terms of motivations, there has been an ongoing concern that cryptocurrencies and other privately issued digital currencies may supersede or even replace Central Bank money (Engert and Fung 2017). Therefore, a major argument for the implementation of CBDC has to do with the rising threat of privately issued currencies, which might not only undermine the Central Bank's monetary sovereignty but also be detrimental to financial stability (Kiff et al. 2020). A CBDC would therefore be a counter-reaction for cryptocurrencies.

Furthermore, it is more complex to supervise and regulate privately issued digital currencies, and thus Central Banks have been nudged to launch CBDCs to mitigate possible economic repercussions and simultaneously ensure compliance with AML/CFT policies to inhibit criminal activity (Bennet et al. 2022).

Another aspect related to the role of the Central Bank has to do with its seigniorage revenue. Seigniorage, according to Engert and Fung (2017, 2-3), may be defined as "*a function of the value of banknotes outstanding (multiplied by the prevailing interest rate, fewer costs of note production and distribution)*". As there is a decline in the usage of cash and physical banknotes around the globe, it is natural that the Central Bank's revenues from seigniorage drop

accordingly. The main problem is that a considerable decrease in the Central Bank's seigniorage revenues may lead to a necessary intervention from governments in terms of funding, which weakens the Central Bank's autonomy (ibid). Thus, in a world that is becoming gradually more cashless, CBDC may be vital to enhance the usefulness of Central Bank money to society, since it enables Central Banks to exert more control over monetary policy and to gain seigniorage (Alwazir, Kahn, and Singh 2022).

Similarly, to privately issued digital coins, Central Banks have been researching the impact that private payment systems may have on the economy. The main threat for Central Banks is that private payments systems may become monopolies not only due to the robust economies of scale and scope but also due to network externalities associated with their business model, which may lead to exponential growth if the user community increases over time (Kiff et al. 2020). Therefore, CBDCs might have a crucial role in the payment systems sector and may increase contestability in the markets of retail and large-value payments (Engert and Fung 2017).

Further, a CBDC would foster financial inclusion worldwide, as several studies suggest how a CBDC can promote financial inclusion. Kiff et al. (2020) argue that a CBDC may be the right step to take since a large share of the population in developing economies is unbanked due to banking system concentration and low incentives to implement new technologies. The Global Findex Database (World Bank 2021) also presents data regarding money saving and consumption, mainly the fact that only 25% of individuals in underdeveloped countries used accounts to save money. The implementation of these digital currencies by Central Banks would be particularly beneficial for unbanked households, who would "*have a savings device to smooth consumption and a buffer against macroeconomic fluctuations*" (Murakami, Shchapov, and Viswanath-Natraj 2022, 39) . A CBDC can also help to assist the digitalization of finance by lowering the expenses of issuing and handling physical currency. According to Banka

(2018), the private cost of utilizing cash in Albania and Guyana is 1% and 2.5%, respectively. Because the accompanying expenses are borne mostly by banks, enterprises, and households, the cost of creating and handling cash in the economy would fall as a CBDC would inherently reduce the demand for paper money (Agur, Ari and Dell' Ariccia 2021).

Nevertheless, some literature supports the opposite thesis. There is the possibility that CBDCs add an unintended element of complexity to the use of mobile money, which subsequently leads to a feeling of uncertainty from consumers regarding the usefulness and the perceived ease of use of the technology (Allen, Cooper, and Esser 2019).

Furthermore, the design of a CBDC, which plays a crucial role in meeting diverse policy objectives, may affect not only financial stability but also bank intermediation, mainly when competing with bank deposits (Fernández-Villaverde et al. 2021). In addition, a poorly designed CBDC may hasten the run-on banks by providing an easily accessible and secure alternate solution to deposits (Mancini-Griffoli et al. 2018).

According to Rennie and Steele (2021), a CBDC could potentially bring privacy risks for CBCD users, that, if poorly designed, can result in a variety of losses, including individual control, liberty, and regulatory control. As a result, it is essential to carefully analyze legal and institutional requirements to comply with applicable international standards.

The implementation of a CBDC might be costly and detrimental to its reputation. It would need CBDCs to become involved in numerous stages of the payment value chain, such as dealing with clients, designing front-end wallets, selecting, and maintaining technology, etc. Failure to carry out these responsibilities owing to technical malfunctions, cyberattacks, or even human mistakes may jeopardize the Central Bank's credibility (Mancini-Griffoli et al. 2018).

In addition, the issuance of a Central Bank bond could also pose competition to commercial banks, as the introduction of a close equivalent for bank deposits could encourage banks to raise deposit rates, resulting in a shift from deposit funding to wholesale funding

(Olsen 2018). Olson also points out that lower economic growth could result in a Central Bank becoming a direct competitor to payment service providers, and banks could therefore lose profit.

Lastly, the introduction of a CBDC could also have risks for international spillovers (Mancini-Griffoli et al. 2018). Currency exchange in countries with high inflation and floating exchange rates could be facilitated by the availability of reserve currency countries' CBDCs across borders (ibid).

To sum up, the motivations and risks hinge on its design and particular circumstances of the country-specific features. Emerging economies have a broader range of reasons, particularly when a CBDC intends to supplement or substitute cash. It is unknown if Central Banks prefer decentralized versus centralized governance systems, as well as what design decisions they make (BIS 2021).

1.1.3 Initiative around the world of CBDC projects

According to the Atlantic Council's CBDC tracker, 112 nations are exploring the possible introduction of CBDCs (AC 2022). Of these, more than 50 countries are at an advanced stage of exploring digital currency (development, pilot, or launch), as of September 2022 (ibid) (Table I). In addition, most banks focus on a widely accessible retail CBDC (47), compared with only a minority of Central Banks developing a wholesale CBDC (9). Twenty-one countries have chosen to work on both, while thirty-four countries are still undecided. Eleven countries have already introduced their digital currency, among them the Bahamas (Sand Dollar) or Nigeria in Africa (eNaira) (ibid).

Some countries are further along than others, such as Sweden in Europe or China. China's Central Bank, the People's Bank of China (PBC), has been actively testing and giving away its digital yuan. As the status of certain countries, particularly China and Sweden are highlighted in some parts of each chapter, this section provides fundamental background of the jurisdictions noted above.

The e-Krona project in Sweden has promoted the use of Central Bank currency, as the project was initiated by Sverige's Riksbank in early 2017 and has proven that a CBDC can successfully complement the existing cash currency. For Sweden, the environment for a CBDC is favorable compared to other countries in Europe, as only 1% of Sweden's GDP product consisted of banknotes in 2018, and banknotes and coins are declining rapidly (Riksbank 2021). This is unprecedented among developed countries, as in comparison to the Eurozone, the GDP was 11% (Fulton 2020). According to the Riksbank, cash is mainly used for small purchases such as coffee or for the elderly (Riksbank 2021). After issuing three reports on e-krona in 2017, 2018 and 2021, the Riksbank pursued its research in 2022, examining, among other things, the impact of e-krona on the economy, the role of the Central Bank, the technical solution, or the significance for Swedish legislation (ibid).

In the meantime, China has continued to invest significant efforts in the development of CBDC since 2014, with the goal of becoming the largest economy to adopt a state-owned digital currency (Deng 2020). Deng (2020) further elaborated that after Facebook issued Libra in 2019 to combat digital currency challenges, China accelerated its research of e-CYN. China introduced its e-CNY as a pilot program in four cities in April 2020 and expanded it to twenty-eight cities in August 2020 (Aysan and Kayani 2022). The environment in China is also convenient for the adoption of new digital payment methods, as 80% of payments in China were processed via mobile payments in 2019 (Gong et al. 2020). China chose to issue E-CYN using a two-tier method (ibid). In the July 2021 People's Bank of China report, the PBoC identified the following objectives for the creation of the e-CYN: 1. Satisfy public demand for digital cash and promote financial inclusion 2. Support fair competition, efficiency, and security in retail transactions 3. Replicate the international initiative and drive the improvement of cross-border payments (PBoC 2021).

1.2 Research Questions

The study's objective is to conduct an analysis of CBDCs in three areas of research: economics, technical design, and privacy in CBDCs. Therefore, the study is subdivided into three sub-RQ derived from the overall RQ presented below:

CBDC – a Matter of Time: Challenges and Implications for Technical Design, Financial Stability and for Privacy, Illicit Financial Activity

Sub-RQ one: Economic Implications of CBDCs - how can CBDCs Influence Monetary Policy Effectiveness and the Financial Stability Goal of Central Banks?

***Sub-RQ two*:** Design Implications and Challenges of CBDCs – how to Develop an Optimal Retail CBDC?

***Sub-RQ three**:* Implications and Challenges of CBDCs Privacy – how to Safeguard Consumer Privacy Without Facilitating Illicit Financial Activity?

The first sub-RQ aims to answer how a CBDC can influence monetary policy and the financial stability goal of a central bank. The second sub-RQ provides an overview of the various design considerations for a retail CBDC and comments on an optimal retail CBDC (r-CBDC). The third sub-RQ focuses on CBDCs privacy and how to protect consumer privacy without allowing illicit financial activity. To achieve this purpose, but also to adequately fulfill the research objective of the paper, the study is divided into three distinct chapters. Each chapter is focusing on addressing one of the following sub-research questions. It is important to note that the delimitations for each chapter are listed separately, as the same conditions and limitations do not apply for each of the above-mentioned sub-research topics. It is also to outline that this paper solely focuses on r-CBDC utilized for daily payments by the general public, as the wholesale- CBDC is limited to the banking industry, which is not in the scope of our study. Moreover, this scenario of a r-CBDC appears to be the preferred option of Central Banks currently considering issuing a CBDC. In addition, most of the literature has analyzed a r-CBDC (Bech et al. 2020; Mancini-Griffoli et al. 2018).

1.3 Disposition

The first section of the thesis is introductory and delivers the background of the research area. The theoretical framework pertinent to the study subjects is discussed in the subsequent chapter. Chapter three describes the research methodology and approach used to address the research questions. The three subordinate research questions are further discussed in Chapters four, five, and six. Finally, Chapter seven summarizes the study's conclusion, scientific contribution, and recommendations for further research.

Chapter 2: Theoretical Background

The following chapter outlines the main concepts, definitions, and stakeholders that are relevant to the research questions. Thus, the chapter begins with an overview of the concept of money and legal tender, followed by cash usage. For the understanding of a CBDC, it is first relevant to define money and its fundamental functions and characteristics.

2.1 Monetary system

2.1.1 Concept of money, legal tender, and cash usage

Money

It is quite challenging to define money in a complete way, such that its definition not only includes the various functions and characteristics it holds, but also adapts to changes over time. Laidler (1969) believed that some people perceived money as a very traditional concept, mainly in the form of physical currency that was held by society, alongside commercial bank demand deposits. A more recent definition by Encyclopedia Britannica (2022, par. 1) states that money "*is a commodity accepted by general consent as a medium of economic exchange*".

In a general way, most of the literature and financial authorities agree that there are three main functions of money. Firstly, it is considered a medium of exchange that enables the effective trade of commodities and services between individuals, such that there is not a shift to alternative exchange systems where one commodity is traded for another (Shirai 2019). Secondly, it is important to mention the unit of account function. In fact, money allows goods

and services' value to be indicated in a standardized, trusted way, such that consumers can easily compare and transact them (ibid). Finally, the store of value function is related to money's capacity to keep its value in the future, such that people can save it to finance future spending (ibid). Plus, this function allows consumers to protect against possible future disruptions in the available income (Fritsche and Größl 2007).

Legal Tender

According to The Royal Mint (n.d.), the United Kingdom's official institution responsible for coin production, legal tender status entails that any payment made in that type of money must be deemed sufficient for discharging a debt. Nevertheless, what is considered legal tender depends on the different jurisdictions. For instance, Article 128 of the Treaty on the Functioning for the European Union (EU 1957, 1) emphasizes that the only notes that can be considered legal tender in the European Union are those issued by the Central Bank or the national Central Banks. The United States Code (1926, Title 31, § 5103) affirms that the country's "*coins and currency are legal tender for all debts, public charges, taxes, and dues*".

An official European Commission Recommendation (2010) states that the concept of legal tender should be fundamentally related to three pillars: mandatory acceptance (unless otherwise agreed between the parties), acceptance at full face value (the amount indicated in the coin/note being equal to its monetary value) and ability to discharge the debtor from the payment obligation.

Even though most jurisdictions consider the respective coins and banknotes as legal tender, some countries have extended the scope of the concept, such as El Salvador and the Central African Republic, which have officially adopted bitcoin as legal tender alongside the local currencies.

Cash usage

The European Central Bank (ECB) has recently published a working paper series where it claims that *"Central Banks, including the ECB, regularly monitor consumer payment habits*

with surveys, in order to be able to identify obstacles which may hinder the smooth functioning of the payments market and future innovation" (Kajdi 2022, 2). The same document contains a survey where only 22% of the respondents said they would prefer (physical) cash if the respondents were offered different payment methods in a store, with 55% stating they would go for a card or another cashless payment (ibid).

Similarly, Panetta (2022) states that cash usage is declining and presents the case of the Netherlands as a clear example, a country where the share of retail payments made in cash dropped from roughly 70% in 2010 to around 25% in 2020 (Figure I). Even if these results were impacted by the Covid-19 pandemic, the expectation is that, by 2025, the share of total transaction value linked to cash payments will be equal to 9.8% only (FIS 2021).

Most literature and studies on the topic of payment methods converges on the same conclusions. As referred above, there is a general belief that cash usage will decline even more soon, which means that other payment methods will become more significant on a global scale. The next era of payment methods will be characterized by *"mobile penetration and the accelerated adoption of digital and contactless payments"* (FIS 2021, 58), with innovations such as digital wallets filling in the void left by the cash usage decline.

2.1.2 Central Banks

Central Banks and the Dual Mandate

A Central Bank is an independent institution whose main responsibilities are to "*maintain monetary and credit conditions conducive to a high level of employment and production, a reasonably stable level of domestic prices, and an adequate level of international reserves*" (Encyclopaedia Brittanica 2019, par. 1).

The creation of the world's first Central Bank takes us back to 1668, the year in which Sweden's Riksbank was founded by the country's Parliament. In line with the goals of current Central Banks, the Riksbank, at the time of its foundation, defined price stability as one of its main responsibilities, stating that it was their main task to "*maintain the domestic coinage at*

its right and fair value" (Riksbank, n.d.). As of today, most Central Banks share a "Dual Mandate" in terms of responsibilities. The US Federal Reserve focuses on price stability and maximum employment (B. Friedman 2008). The European Central Bank also focuses on price stability, but its second goal is directed towards supporting general economic policies in the European Union (Ioannidis, Murphy, and Zilioli 2021). Even if defined in a different way by each Central Bank, one can assume that the Dual Mandate is, in general, associated with monetary and financial stability (Moenjak 2014).

The different functions of Central Banks

Central Banks' functions can be divided into five major pillars (Moenjak 2014).

Firstly, Central Banks are responsible for the issuance of money in the economy. In other words, these independent institutions make decisions regarding the quantity of money in circulation, such that the economy can run in a smooth way (Ajayi 1999). The Central Bank money that is issued not only includes coins and banknotes, but also an electronic form of money when Central Banks directly credit commercial banks' accounts held at the Central Bank itself (Moenjak 2014). Furthermore, Central Banks benefit from exclusivity in terms of cash issuance with legal tender status, which is directly linked to their influence on the real value of the respective currency, that is, its purchasing power (Iwańczuk-Kaliska 2017).

Secondly, Central Banks are responsible for the safety and infrastructure of payment systems. Iwańczuk-Kaliska (2017, 77) defines three pillars of Central Banks' responsibility of payments systems, which include being an "*oversight authority, a catalyst, and an operator*".

Additionally, Central Banks may need to step in as Lenders of Last Resort. In fact, under heavy economic turmoil, Central Banks might need to intervene to meet the "*abnormal increase in demand for liquidity which cannot be met from an alternative source*", mainly by providing urgent liquidity to financial institutions under severe financial distress, or even to the market (Freixas et al. 1999, 64). The increased risk borne by Central Banks when intervening as lenders

of last resort entails not only the payment of a relatively high interest rate by the illiquid bank to the Central Bank, but also the implementation of a haircut in collateral value (ECB 2019). Central Banks are also responsible for being active supervisors of the banking system, mainly be engaging in macro-prudential supervision (Iwańczuk-Kaliska 2017). In general, banking supervision entails those authorities engage, with operational independence, in the creation of a safe banking environment under which banks can effectively operate with a sufficient level of reserves and capital to meet their respective risk profile (BCBS 1997).

The final function of Central Banks is monetary policy implementation. Article 127 of the Treaty on the Functioning of the European Union (EU 1957b, 1) declares that one of the essential tasks to be executed by the European System of Central Banks is to "*define and implement the monetary policy of the Union*". In the case of the United States of America, three principles are essential for monetary policy implementation: adjusting the policy interest rate to meet the 2% inflation target, allowing for a general understanding by the society of the impact of the different policies and take into account the possible implications of events that will have an impact in the long term, even if not in the short-term (FED 2018).

Monetary Policy: conventional vs unconventional mechanisms

Conventional monetary policy mechanisms generally entail the formulation of a target for the "*overnight interest rate in the interbank money market and adjusting the supply of Central Bank money to that target through open market operations*" (Smaghi 2009, 2). These operations usually entail a marginal lending facility and a deposit facility, both overnight and with their respective facility rates (Whitesell 2006). This means that banks can make overnight deposits at the Central Bank and get paid the deposit facility rate, which sets the floor for the interbank rate, or borrow money overnight and be subject to the payment of the marginal lending facility rate, which sets the ceiling for the interbank rate (Bindseil and Fotia 2021). Setting these interest rates represents a vital role of Central Banks in the context of conventional monetary policy.

However, conventional mechanisms may not be effective or even possible under certain circumstances. When the policy interest rate reaches the zero lower bound, Central Banks need to resort to unconventional measures, whose purpose is usually associated with changing the size and composition of the Central Banks' balance sheet and to affect the expectations on the "*medium to long-term interest rate*" (Smaghi 2009, 3).

Quantitative Easing

Quantitative easing is an unconventional instrument of Central Bank monetary policy often used to increase the supply of money through *"large-scale asset purchases"* (mainly long-term ones, such as Government bonds) to *"inject money into the economy in order to revive nominal spending"* (Bedford et al. 2009, 90-91), and is commonly adopted in times of turmoil in financial markets and/or profound recession (Belke, Gros, and Osowski 2017). In fact, this instrument of unconventional monetary policy fosters investment and consumption by reducing long-term interest rates, whereas standard monetary policy is generally aimed at decreasing short-term interest rates (Gagnon 2016). Under a Quantitative Easing policy, Central Banks fund their asset-purchase by issuing reserves, thereby expanding their balance sheets on both sides, that is, assets and liabilities (G. Benigno and P. Benigno 2022).

Helicopter Money

Helicopter Money is another unconventional instrument used to conduct monetary policy. The idea was first mentioned by the Nobel laureate Milton Friedman, who described this unconventional mechanism as if a helicopter was flying over people dropping "*bills from the sky*" (Friedman 1969, 4-5). Ben Bernanke believes that helicopter money becomes relevant in a context of high levels of government debt, since the tax cuts that allow money transfers to households are money-financed rather than debt-financed (as it happens with pure fiscal policy) (Bernanke 2016). This policy started as a thought experiment from Friedman, however, in reality, it consists of an increase in the monetary base from the side of Central Banks which

finances the expansionary fiscal policy of Governments, which entails either a tax cut or a public spending increase (ibid). Helicopter money in the form of direct transfers from Central Banks to individuals, that is, money creation directly transferred to the economy (Fiebiger and Lavoie 2018), becomes relevant in the context of CBDCs, mainly when referring to CBDC accounts held at the Central Bank.

2.1.3 Commercial Banks

According to the National Information Center of the U.S. Federal Reserve, commercial banks tend to take part in different lending activities and are profit oriented (NIC, n.d.). These financial institutions play an essential role in the economy, with regard to financial stability and the financial services provided to the public, which include the lending activities mentioned above and other services. The main functions of commercial banks entail deposit-gathering and grating loans to households and businesses, besides engaging in "*lending for infrastructure, real estate, and other projects*" (IFRS 2022, 144).

Commercial banks are also an important pillar of the money creation process. Greenham et al. (2011, 1) state that commercial bank money is created under three circumstances: (a) when commercial banks grant a loan and create a deposit account for the borrower; (b) when using customers' overdraft facilities to make payments on their behalf and (c) when they make payments on their own behalf to buy assets from the private sector. Plus, commercial banks' activity is inherently related to the concept of maturity transformation, since these financial institutions rely on short term liabilities (mainly short-term deposits) to fund the investment on long term assets (mostly long-term loans) (Entrop et al. 2015; Paul 2022).

2.2 Blockchain

Blockchain is a disruptive and revolutionary technology that has far-reaching implications in various areas, in particular the banking sector where it is supposed to alleviate the reliance on a centralized trusted authority (Counsell, Dashkevich, and Destefanis 2020). Recently, different

proposals for the application of this novel technology started to emerge, inter alia the exploration of blockchain-based retail CBDCs (Che et al. 2022).

According to the PwC CBDC Global Index (2021), the underlying technology of blockchain is examined in more than 88% of the recent CBDC projects. However, Central Banks currently face difficulties in selecting the appropriate design for issuing retail CBDCs due to practitioners' and academics' lack of scientific treatment (Chen et al. 2018). In the following section, the theoretical background of blockchain is studied and explained. Additionally, technical, and conceptual principles have been outlined to draw a better understanding of the potential impact on current and future payment methods and the financial market infrastructure.

2.2.1 Characteristics of Blockchain

Blockchain, a subset of Distributed Ledger Technology (DLT), is a protocol with a set of rules that governs the operating network system (Chen et al. 2018). It enables peer-to-peer (P2P) value transactions without the involvement of a central authority, which means that multiple independent entities share control of the entire ecosystem.

The network comprises nodes (computers), that record transactions based on mutual agreements. Each peer carries a copy of the record on a ledger to keep the P2P network completely decentralized and secure. This ledger can be regarded as a database or digital file of written records of transactions (Mell et al. 2018). These transactions are collected in chronological order in so-called blocks that respectively consist of block header and data (Ma, Ren, and Wang 2022). Table II demonstrates the verifying and execution processes of blockchain transactions. After successfully validating the transaction requests by the nodes, the block is added to the chain. This guarantees that a copy of the most recent ledger is always available on every node in the network, which makes the system robust and resilient (Group of

Central Banks 2021). Furthermore, a summary of blockchain fundamentals is shown in Table II.

Asymmetric Cryptography

Asymmetric Cryptography, commonly referred as Public-Key Cryptography (PKC), is the underlying principle used in blockchain technology; it uses different keys to encrypt and decrypt messages. Cryptocurrencies such as Bitcoin apply this fundamental PKC framework for transactions that are based on the Unspent Transaction Output (UTXO) model (Chakravarty et al. 2020). It allows users of the network to initiate on-chain functions such as sending and receiving funds without having a third party involved to verify the transaction requests (Hellman 1978).

As prior mentioned, there are pairs of keys, public and private mathematically related and used to encrypt or decrypt transaction data. This cryptographic system is called "asymmetric" since both keys are different from each but are needed to access any encrypted information (Adleman, Rivest, and Shamir 1978). The public key, which is open to everyone in the network, allows receiving transactions while the private (secret) key requires the owner to unlock the address and access the funds (Antonopoulos 2014).

Additionally, to transfer value on a blockchain, it is required to digitally sign the document that verifies the authenticity of the sender's transaction; it is equivalent to an in-person signature (Hellman 1978). It also serves the purpose of data integrity and non-repudiation, hindering the ability of the sender to refute having sent the message (Agrawal and Verma 2013). Lastly, one must ensure that sufficient funds are stored in the wallet. This is done by reading the target of the transaction output, the public address, that is accessible to the entire network.

Smart Contracts

Smart contracts are computer programs or digital agreements embedded in a blockchain or distributed ledger. These non-custodial protocols include so-called "if-then statements" that run self-automatically when pre-programmed conditions are met (Nick 1994). This emerging technology has various use cases, particularly the adoption of Decentralized Finance (DeFi), which challenges the current centralized banking system (EU Blockchain 2022). The inclusion of encrypted digital rules ensures fast and secure execution of transaction requests without the involvement of a middleman and their associated time and fees (Fong et al. 2021).

These digital rules are immutable and append-only, thus specific conditions can only be modified by overwriting the agreement without altering the existing statements (Andesta, Faghih, and Fooladgar 2019). According to Bechtel et al. (2020), smart contracts have the potential to support new digital economy applications such as programmable CBDCs by enabling their issuance as a new form of money and facilitating payment and settlement processes. Some Central Banks such as PBOC already tested the e-CNY with smart contracts features to accelerate the process for after-school training programs (Wahid 2022). Additionally, Riksbank is exploring the potential integration of smart contracts into the e-Krona payment system (Schickler 2022). Central Banks, however, are aware of the implementation coming with a set of risks and that software bugs may negatively impact the platform's security.

2.2.2 Types of Blockchain Networks

Various types of blockchain networks differ mostly in data publicity and network governance (Vitalik 2015; Chen et al. 2018). In principle, current blockchain systems can be primarily categorized into *(1) public, (2) private, and (3) consortium blockchain.* An overview of the main blockchain types is shown in Table III.

Public Blockchain

Public blockchains are completely decentralized and permissionless. This means that no individual or group manages the network; everyone is allowed to read, write, and audit ongoing transactions without any restrictions (Strehle 2020). Additionally, users of public blockchains are not required to divulge their identity, however, network participants can view the transactions made by the respective wallet address (Nakamoto 2008).

The security of the network depends on the number of nodes; thus, financial incentives in form of rewards are granted to participants to verify transactions and mine new blocks. This process makes the system more resistant and mitigates the risk of a so-called "51% attack" by a conglomerate of miners who owns more than half of the network computing power or hash rate (Al-Ahmad et al. 2022). Lastly, anyone can access the network from anywhere which makes it more accessible compared to traditional banking systems. To regulate the access of network participants, the subsequent blockchain is used (Dlodlo, Ncube, and Terzoli 2020).

Private Blockchain

Private Blockchain networks are centralized and permissioned. This enables a single organization to have more control over its network by deciding on the gatekeeper which executes the consensus protocol and maintains the shared ledger. Furthermore, the central entity can restrict access to the operating network which leads in general to a much smaller network size compared to a public blockchain (Brousmiche et al. 2017). To ensure the eligibility of the network user and increase trust within the system, the identity of each participant is verified and validated by the network operators or by smart contracts (Dlodlo, Ncube, and Terzoli 2020). Lastly, the private blockchain is much faster regarding scalability and processing speed due to the limited number of users. The nature of private blockchains, however, leads to a higher prone of security threats such as fraud and bad actors (Kogan and Wang 2018).

Consortium Blockchain

The consortium blockchain is an extension type of the private blockchain which attempts to remove its sole autonomy. More than one pre-selected authorized node is responsible for making the best decisions possible for the network's utilization as a whole. These collections of nodes are designated as consortia or federations (Brousmiche et al. 2018).

The function of a federated blockchain can be illustrated by the simple case example: If one assumes a consortium of 20 financial institutions where transaction requests are confirmed by 15 out of 20 authorized nodes, the decision is deemed to be right within the network if 75% of the federation confirms. Lastly, consortium blockchains are more cost and energy-efficient with regard to transactions compared to public blockchains (Chao et al. 2019).

2.2.3 Consensus mechanism

Various consensus mechanisms serve the purpose to ensure the validity of transactions, differencing only in the *way* they reach consensus. The most common consensus mechanisms are *Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and lastly Proof of Authority (PoA).* Due to their prevalence, this paper will focus on PoW and PoS.

Proof of Work (PoW)

The most common consensus algorithm is the PoW model, applied among others by the Bitcoin network. However, it is said to be the most inefficient concept to achieve consensus as it requires a considerable amount of computational power to solve the complex mathematical equation called a hash (Agung et al. 2019). After solving the problem by one node, also known as a miner, the new block is added to the chain and copied to every node which is essential for network security (Capkun et al. 2022). Due to the amount of energy consumed by miners, new consensus models have been explored to make the system more scalable and environmentally friendlier.

Proof of Stake (PoS)

The next most popular consensus algorithm is PoS which has frequently been compared with PoW because of its scalability and efficiency advantage. Both use economic resources to gatekeep the level of participation in the network. However, this consensus protocol does not require an excessive amount of electricity consumption for transaction validation since it uses a method called "staking" (Azmathullah, Rizwan, and Sheikh 2018). This means that the protocol chooses the next block to be appended to the chain, based on the current "stakes" which represent total cryptocurrency tokens held by the validator for some time during their service. The higher the stake percentage of the network node over the entire network, the higher the probability to be chosen as a validator. After "forging" the new block, the validator is rewarded with transaction fees like other consensus algorithms (Fanti, Kogan, and Viswanath 2019).

Delegated Proof of Stake (3) and *Proof of Authority (4)* are alternatives to the aforementioned consensus algorithms. The DPoS is similar to the preceding PoS algorithm with the distinction of being a more efficient and democratic version. Stakeholders vote for delegates, also known as witnesses, who are then responsible for validating the new blocks (Long et al. 2019). PoA is designed to be used in private blockchains due to its centralized nature. A small group of authorities are pre-approved and serve the role of transaction validators due to their identity or reputation staked in the network. This significantly increases the speed of validating the transactions (Manolache, Manolache and Tapus 2021).

2.3 Key platform components for a retail CBDC

This short paragraph illustrates from a high-level technical perspective the key platform component required to ensure the reliable transfer of CBDCs to the end-users on the example of a hypothetical model made by Bank of England (Figure II). The underlying platform infrastructure on which the CBDC is operated on consists of *End-Users, Payment Interface*

Providers (PIP), Application Programming Interface (API), and *the Central Bank Core Ledger* (Bank of England 2020).

Firstly, providing ***End-Users*** intermediated access to the payment system illustrated in the basic model requires the equipment of the general public either with mobile wallet applications (in case of a token-based approach) or, in case of an account-based approach, with accounts held by the Central Bank (Agur et al. 2018). These are the two most common perspectives to be discussed later in more detail. In the model proposed by the Bank of England, the end-user is accessing the Central Bank accounts over an intermediary and not directly with the Central Bank. This indirect architectural model is in accordance with many current pilot and research projects such as the e-Naira from Nigeria and the e-CNY from China (Central Bank Nigeria 2021; PBoC 2018). As opposed to the indirect model, Sand Dollar (Bahamas) follows a direct model approach (Central Bank Bahamas 2019).

Payment Interface Providers (PIPs) are authorized and regulated intermediaries that are said to provide user-friendly interfaces between the end-user and the core ledger (Group of Central Banks 2020). It is in principle a database that records all monetary transactions conducted within the operating system (World Bank 2017). End-users are obligated to understand the usage of the interface which requires intensive education and a lot of resources. However, this is essential for a successful implementation and mass adoption of digital currencies. Furthermore, private sector companies can add functionality and design features, so-called "overlay services", to make CBDC more convenient for the end-user (Bank of England 2020). In this case, the role of PIPs would also include the assurance of legal compliance with know-your-customer (KYC), combating financing of terrorism (CFT) and anti-money-laundering (AML) regulations. Thus, customer due diligence as well as user and transaction verifications are required to be conducted in a thorough way (Central Bank 2020).

Lastly, connecting the ***Payment Interface Provider*** with the ***Central Bank Ledger*** requires a so-called CBDC API, (Application Programming Interface), which is basically a software intermediary that allows only regulated and authorized entities to access the ledger and conducts secure payment instructions (IMF 2020). The Central Bank Ledger processing primarily the payments could be based either on a centralized or distributed ledger by using distributed ledger technology (DLT). A payment network based on DLT would remove the need for a trusted third party, making the system more reliable and resistant to hackers since the same data is stored on multiple computers (Gross et al. 2020).

The validation process of each financial transaction, recorded as a block, is conducted by network nodes, which can be described as electronic devices connecting to the blockchain network. Depending on the consensus protocol, which describes how peers come to an agreement, the validation process can have different outcomes. This can lead to acceptance or rejection of certain transactions based on predefined rules (Huang and Zhang 2022). There are some advantages in using DLT, however, some research studies question the necessity of using this technology in a centralized issuance system (National Bank of Ukraine 2019; Sverigies Riksbank 2018).

2.4 Comparison: Cryptocurrencies and Stablecoins

The emergence of cryptocurrencies such as Bitcoin and Ethereum has experienced exponential growth over the last decade as an investment and means of payment. It has modified and revolutionized the economic and social environment with new expectations on available digital forms of payments. They are built on the premise of decentralization; neither Central Banks nor public authorities are issuers, which imposes stability concerns (IMF 2022). Christine Lagarde, president of the European Central Bank, regards cryptocurrencies as highly speculative and does not consider them as an official currency (Browne, 2022).

Moreover, as of today, Bitcoin is not accepted as legal tender and is even banned by

some Central Banks. As previously mentioned, El Salvador is the first country to recognize Bitcoin as legal tender, followed by the Central African Republic (CAR) (IMF 2022). The motivation behind the country's decision was to make payment transfers cheaper, drive financial inclusion, and be less dependent on the inflation of the US dollar (Bukele 2021). Nevertheless, there are some associated risks and downsides with using cryptocurrencies such as the notorious price dynamics that may result in financial instability. Besides the tremendous price volatility, there are major issues with liquidity and regulation around the crypto market which have led to the development of stablecoins, most of which are pegged to USD (Lyons and Natraj 2020).

As opposed to volatile digital assets, these types of coins aim to achieve constant or stable value to offer investors protection from intense price fluctuations. Thus, the value is designed to be pegged to an existing asset such as fiat currencies or exchange-traded commodities that might serve as a means of payment. The most prominent stable coin projects based on market capitalization are Tether (USDT) and USD Coin (USDC); both are fiat-pegged to the U.S. Dollar (Baur and Hoang 2021). Although stablecoins are supposed to be stable, the Terra project's failure in May 2022 proved that it is not always the case; it lost its peg to the U.S. dollar and collapsed (Aste et al. 2022). In the recent Digital Euro Summit 2022, industry experts shared the view that privately issued stablecoins are not subject to regulatory safeguards yet. Thus, it cannot be an effective medium of exchange; death spirals may occur where coins become worthless (Attanasio et al. 2022). Consequently, it is proposed for instance by Miguel Ordonez, former Governor of the Bank of Spain, and member of the Governing Council of the ECB, to issue the private sector stablecoins and back them with treasuries and Central Bank reserves (Ordonez 2022). The European Commission distinguishes between "asset-referenced tokens" and "e-money tokens". The former token is supposed to be pegged by several fiat currencies, commodities, or a combination of both, while the latter token refers only to one fiat

currency as a legal tender (European Commission 2022).

In terms of crypto regulations, the first cornerstone has been set out by the European Union (EU) with the MiCA framework which focuses on transparency, clarity, and consumer protection with digital crypto assets (Mclaughlin, Morgan, and Zhang 2022). Lastly, the pressure increases for Central Banks due to the dominance of U.S. dollar-denominated stable coins, and recently private payment service providers such as Apple pay started allowing paying with USDC. This is regarded as a call to action.

Chapter 3: Methodology

3.1 Research Method

In each chapter, a literature review is conducted first, which builds the foundation for the structured interview questions and provides introductory context and comprehension of the topics presented above.

3.1.1 Aim of interviewed experts

The objective for the experts is to evaluate on the findings presented in the literature of the individual chapters. The primary focus is on gaining further insights and identifying certain commonalities while also naming the distinctions to the scholarly view. The results of the interviews are also analyzed and interpreted. As an empirical analysis is not yet possible at this stage and is also outside the scope of our work, the work draws on expert knowledge. The main purpose of this research is to gain a realistic view as possible, generated by the analysis of interviews with top experts in the financial technology and payment fields.

3.1.2 Structured interview

Since empirical analysis is not feasible at this stage, expert knowledge is used to answer the research questions appropriately. The empirical investigation is conducted in the form of a structured interview guide, which is done based on an elaborated guideline with open questions. A structured interview contains a set of standards that the researcher must strictly follow

(Stuckey 2013). According to Castillo-Montoya (2016), an interview protocol is a tool used by a researcher to ask questions to obtain information relevant to the study objectives.

In this respect, the guided expert interview is a form of qualitative interview and, thus qualitative research method with a partially standardized character. This ensures clear goal orientation and comparability of results by answering mandatory questions. Bell and Bryman (2006, 28) describe qualitative research as *"a research strategy that usually emphasized words rather than quantification in the collection and analysis of data"*.

In addition to the welcome and closing sections, the guide consists of three sets of topics that are addressed in particular in the individual chapters. To accommodate the fact that both bank representatives and lawyers or other experts in the field of CBDC are involved in the interview, the guide is adapted according to the interview group in order to meet the respective perspectives. The content of the guide will be derived from the main points mentioned in the individual chapters. Furthermore, two methods are used to answer the questions in the corresponding block of questions: the qualitative method and the quantitative method, which are regarded as complementary rather than opposing methods (Roberts 2002). Roberts further argues that the qualitative and quantitative research methods are being in continuation of each other. Open-ended questions are used as a qualitative tool to obtain the most comprehensive and uninfluenced response possible (ibid). The expert is expected to answer the questions in his or her own word. The responses are categorized in the subsequent evaluation. As a quantitative instrument, experts are asked to assess specific, identified implications, statements, or challenges on a five-point scale. In the case of extreme evaluations, the expert is explicitly asked for a corresponding explanation.

To ensure a common understanding, key terms are defined before the respective questions. The first block of questions deals with general questions about the person and the profession, followed by questions on the respective sub- research question.

3.1.3 Expert selection

Based on the underlying research questions, experts are selected from the fields of Central Bank coins, digital money, blockchain, or other related fields. The picked experts are bank advisors or members of the governing board with a focus on Central Bank money and payment experts as well as emerging technology experts, e.g., from the "Big Four" corporations, and lawyers who are representatives in this field. To avoid saturation at an early stage, participants from fields other than financial technology were chosen.

However, it should be emphasized that interviewing the same experts for each chapter was not practicable because some questions could only be addressed by specific specialists in the relevant industry and the appropriate expertise. Therefore, tables were created for the respective chapters to explain more detailed information about the experts interviewed (tables IV, V and VI). The researchers contacted the experts exclusively through their professional and private networks. There needs to be a careful assessment of the question of how many experts are optimal. Four to five candidates were chosen as final participants for each chapter of the thesis. Due to the scope of the thesis, there was an oversupply of experts with similar professional backgrounds and current professional positions, despite more than four or five participants having an acceptable comprehension of the subject. Consequently, the final selection was narrowed down to four or five experts, depending on the sub- RQ. The specialists chosen are qualified based on their experience, qualifications, and specialized expertise. The experts have been assured that their identities and firms would be anonymized, making it impossible to later link claims to specific persons or corporations. However, some experts have given their consent to the publication of their name. It is important to emphasize that these are personal opinions of the experts, which do not necessarily coincide with the opinions of their institutions and employers. Permission to conduct the interview was also secured during the procedure. The detailed interview questionnaire and reports can be found in the Appendix.

Michelle Bader, 50818

Chapter 6: Implications and Challenges of CBDC Privacy -how to Safeguard Consumer Privacy Without Facilitating Illicit Financial Activity

6.1 Problematization and Research Objective

To this day, cash, which is the only type of legal tender that Central Banks make available to individuals, serves as the most anonymous form of payment (Kahn, Mcandrews and Roberds 2004). The question of a legal tender status of a CBDC has been raised in recent discussions and is seen as complicated (BIS 2018). Cash is a bearer instrument, meaning it does not require the services of an intermediary when transferred from one person to another. There is no record of who makes a cash payment, or when that cash payment was made, meaning it is fully anonymous and most of the time it doesn't leave a trace (Sands et al. 2017). Aside from that, data protection, trust, and privacy are critical components of the monetary system, with privacy identified as a key factor in the development of CBDC (Bech et al. 2020).

In April 2021, the European Central Bank (ECB) published a comprehensive analysis of its public consultation on the digital euro. The ECB conducted a study of 8,221 individuals to determine stakeholder perceptions of a digital euro. The main finding is that people express a strong desire for privacy. The study reveals that respondents value privacy as its most important feature (43%), ahead of security (18%), followed by the ability to pay across the euro area (11%) (ECB 2021). This finding is independent of the respondent's country of origin, socio-demographic characteristics, or socio-economic standing. This result may come as a surprise, but the fact that stakeholders place a strong emphasis on privacy is a consistent outcome in several papers (ECB 2021; Krasnova and Veltri 2010; Shostack and Syverson 2004). A fully transparent CBDC would offer authorities full access to user identity and transaction data, resulting in clear financial integrity supervision advantages unless there are no restrictions on that. A CBDC could raise concerns about digital surveillance, such as a CBDC potentially being instrumentalized against users. One example is consumer profiling by

charging higher mortgage rates to people who purchase alcohol (Mancini-Griffoli et al. 2018). Consumers prefer privacy in CBDCs to avoid multiple challenges, such as being spammed or stalked (Böhme et al. 2022). At the same time, a CBCD should not be used to conceal illegal transactions. A privacy preserving CBDC must comply with legal requirements, notably with anti-money laundering (AML) and combating the finance of terrorism (CFT) regimes, as well as *"Know your customer"* (KYC) standards (Grothoff and Moser 2021). A high standard of privacy may be one of the keys to success for a future CBDC (Bech et al. 2020). Hence, it is essential to find a privacy-enabling solution without enabling illicit financial activity (AML/CTF). Ultimately, this outlines the sub-research question that the chapter intends to explore:

Sub- RQ: Implications and Challenges of CBDCs Privacy – how to Safeguard Consumer Privacy Without Facilitating Illicit Financial Activity?

6.2 Scope and Delimitations

For the understanding of the sub-research question, it is first vital to define and delineate the terms used in this paper, as they partly differ in their definition and meaning. It must be highlighted that the chapter does not aim to explore the global legal problems related to a CBDC. Still, it is relevant to understand privacy and AML/CTF/KYC standards. In addition, this chapter does not represent a comprehensive analysis of the AML/CTF/KYC and other related laws. The chapter targets CBDCs and how they could handle personal privacy with respect to IFA. Because of the scope of the work, the theoretical part's fundamental values are based on those of the European Union (EU). It should be noted that the concept of privacy differs across jurisdictions and may also vary with respect to private versus public actors. The work's scope does not allow a detailed examination of countries that operate in very diverse ecosystems (Bahamas, Venezuela, etc.) with the exception of China. Some literature on China's digital currency handling in terms of privacy and AML/CFT is analyzed. It is to be noted that most literature on CBDC's have dealt with strategic considerations, technology, and economic

analyses (Auer, Cornelli and Frost 2020; Allen et al. 2020; Kumhof and Noone 2018), and all of these *"flag the importance of privacy"* (Böhme et al. 2022, 2).

Prior works have focused on privacy protection for traditional e-payments (Kim et al. 2010; Linck, Pousttchi and Wiedemann 2007). However, CBDCs differ from traditional e-payment systems that are secured by banks or companies such as Mastercard or PayPal.

Privacy is one of the most complex issues in the CBDC debate and probably sparks the most heated discussions (Ballaschk and Paulick 2021). Due to the lack of academic studies on privacy and IFA, the chapter will specifically address this research field to provide input to the existing research on this perspective and contributes to filling this literature gap.

6.3 Theoretical Foundation – Privacy and illicit Financing

In the context of this chapter, it is first crucial to concretize the definition of privacy, as it is one of the fundamental subjects discussed in this chapter. Brunnermeier and Landau (2022, 24) describe privacy as a "*core value for European citizens"*. It is an individual right but also a common and social good (Grothoff and Moser 2021). Privacy builds the basis for many other human rights, such as personal freedom (Banisar 2006). The principles of privacy and personal data protection are codified in law in articles 7 and 8 of the charter of fundamental rights of the European Union (CFR 2007) in the General Data Protection Regulations (GDPR*)* (EP and EUCO 2016), in Article 8 of the Convention for the protection of human rights and fundamental freedoms (ECtHR 1950), as well as in Article 12 of the Universal Declaration of Human Rights (UNGA 1948) *(see Glossary for full definition of laws)*

A further key aspect of the research question addresses illicit financial activities. As per definition, illicit financing is defined as "*money illegally earned, transferred, or used that crosses borders"* (Forstater 2018, 4). Illicit financial flows (IFFs), falls into three main areas, acts that are illegal themselves: corruption, tax evasion, financing of terrorism (Reuter 2017). Therefore, to adequately answer the research question, numerous protection concepts must be

accounted for, including anti-money laundering (AML) and counter-terrorist financing (CTF) regulations. The status of European Central Banks is incompatible with their submission to the AML/CTF legislation, which applies to participants in digital money transfer markets. AML/CTF activities are governed by a legal framework designed to *"protect the financial system from fraud, crime, and political violence"* (Frasher 2016, 1). For the chapter's purpose, *"Know Your Customer"* (KYC) regulations are also included. It is a process for verifying the identification of a customer who is *"willing to onboard an institution to avail its services"* (Malhotra, Saini and Kumar 2022, 1988). KYC is important for institutions like banks and insurance companies to verify their client's involvement in illegal activity (Mondal, Deb und Huda 2016). KYC regulations, under certain circumstances, allow professionals, *"to reveal the identity of counterparties or account holders with the aim of fighting against money laundering"* (Brunnermeier and Landau 2022, 24).

6.4. Analysis of implications and challenges of CBDCs privacy and other policy objectives

This section outlines consumer privacy concerns and addresses the importance of some levels of privacy in CBDCs. It also identifies barriers, such as money laundering or terrorist financing for fully anonymous CBDCs and provides some examples of countries in their use.

6.4.1 Privacy and CBDC: Implications and concerns of consumer privacy

Consumers favor protecting their privacy in CBDCs to avoid being spammed, robbed, or having their identities stolen (Böhme et al. 2022). Böhme et al. further claim that payment records demonstrate an in-depth picture of an individual's behavior. For example, they can reveal information about a person's health or interests. Individuals do not want the burden of deciding whether the information is sensitive (e.g., a person's lifestyle or political learning) or private (Rennie and Steele 2021). *"Consumers may also demand privacy to avoid being tracked by ads as a result of their purchase"*, especially in the digital age (Gardin 2019, 49). Some networks could also forcefully exploit or sell users data to third parties (Brunnermeier and Landau 2022).

Companies could leverage this information to, for instance, engage in price discrimination and extract consumer surplus (Garratt and Van Oordt 2021). Consumers may also want to remain anonymous to avoid signaling their wealth or to protect their reputation.

Rennie and Steele (2021) outline policy choices involved in designing a CBDC and the implications of these choices for individual privacy. They assert that Central Banks have a variety of priorities that could ultimately undermine privacy. They further state that the current CBDC models possess privacy risks to CBDC users that could materialize into losses such as the *"loss of anonymity, loss of liberty, and loss of individual control"* (ibid, 10). Privacy is a critical challenge, and a CBDC will *"expose new forms of sensitive information to CBDC operators"* (Allen et al. 2020, 7). Moreover, a survey conducted by BCG (2018) also reveals that 30% of users believe that companies are not honest with their data. The survey implies that users' concern about data misuse is evident in organizations related to financial, technology, and government services. Consequently, the implementation of CBDC would lead to more privacy and trust concerns. Borio et al. (2017) claim that the main benefit a CBDC could bring is some level of anonymity for electronic payments. Privacy in digital payments may also yield legitimate reasons to stay anonymous. For instance, a consumer with a preexisting medical condition may want to purchase medication anonymously without facing negative consequences from parties such as their insurance. Some consumers may also retain privacy in transactions for unlawful reasons, such as the lack of a government-issued ID (Brunnermeier and Landau 2022). Another benefit of anonymity in CBDC is limiting exposure to hacking (Mancini-Griffoli et al. 2018).

In the country example of China, by law, all residents must accept e-CNY and other digital currencies (Xu 2022). The People's Bank of China (PBC) announced a revision of the PBC Act, highlighting that the digital currency will be formally launched in legal forms of payment and that people will not be allowed to refuse to accept e-CYN if they have suitable

facilities (ibid). One of the main concerns raised by e-CYN detractors in China is privacy (Allen, Gu and Jagtiani 2022; Huang and Mayer 2022). The digital yuan is said to be "more about policing than progress" (Goh and Shen 2019). Because all transactions are 100% trackable, the PBC could monitor and cancel any transactions, including the amount and foreign exchange involved, as well as identify the participants. Fanusie (2020) notes that China may force Chinese enterprises to solely take payments in digital yuan, forcing foreign companies based in China to comply as well. It is said to be that the issue is less about money and more about data (WSJ 2021). He further states that the PBC could set an expiration date for digital money depending on its interests, causing further privacy concerns. That also implies that participants have no control over what will happen to their funds or how and when they spend their money. Moreover, a draft released in 2020 of the public solicitation of comments of the People's Bank of China Law (PCOCL) states that the Central Bank would oversee the establishment of a national financial database, the collection and management of national financial industry data, and the supervisory exchange mechanism with the Financial Stability Development Committee (Cheng 2022). In other words, the notion of "controllable anonymity" would still allow full access to user data and criminal investigations in the future, raising further concerns (Chorzempa 2021).

On the other side, Dupuis, Gleason and Wang (2021) conducted research on CBCD, financial secrecy, and privacy by jurisdiction. The study analyzed 36 nations that intend to implement CBDCs. Among these countries, Sweden has the highest level of personal freedom, and trust in government is among the highest in the world (OECD 2021). In countries where the rights to privacy and freedom are anchored in fundamental documents and legislation, the implementation of CBDC may deliver advantages without causing a significant loss of freedom (Dupuis, Gleason and Wang 2022). Fanusie (2020) added that a fundamental assumption that privacy might not be a major concern is that we live in a liberal democracy with a free-market

economy. That also indicates that Swedish citizens have trust in the current system and that privacy is not a major concern.

Several papers explore whether consumers benefit from revealing their private information or not (Liu, Sockin, and Xiong 2020).

6.4.2 Barriers to full privacy protection in a CBDC

In addition to privacy concerns, there are policy obligations, including anti-money laundering (AML) and counter-terrorist financing (CTF), that must be considered in the design of a CBDC. These are also important factors when addressing the research questions.

From the standpoint of the government, privacy conflicts with other equally valid policy objectives (Brunnermeier and Landau 2022). Central Banks face a trade-off between satisfying user preferences for privacy and mitigating IFA (FED 2022). The Reserve Bank of Australia (2020, 37) has stated that it is not possible for a CBCD to *"fully match the levels of anonymity and privacy,"* as it carries concerns related to the facilitation of the shadow economy and illegal transactions. This finding is consistent in various papers: a fully anonymous digital currency would raise concerns and would not be compatible with regulators' AML/CFT requirements (Ballaschk and Paulick 2021; Gnan and Masciandaro 2018; Mu A. and Mu Y. 2022).

The economic literature has often emphasized two main characteristics of money: its liquidity and the rate of return. Consequently, privacy and money are often analyzed through the lens of the adverse consequences of anonymity, such as money laundering (Rogoff and Woodford 2015). They further point out that *"a large percentage of currency in most countries, generally well over 50%, is used precisely to hide transactions"* (ibid, 447) and stress those criminal activities are prevalent due two key features, anonymity, and convenience. The EU, for instance, is a world leader in the fight against money laundering and the financing of terrorism. Four days before the ECB published its investigation phase of the digital euro, the European Commission unveiled its ambitious package of legislative proposals to reinforce the

EU's anti-money laundering and countering terrorism financing rules, considering the emerging challenges linked to technological innovation such as virtual currencies (EC 2021).

However, according to the Bank of International Settlements (BIS), anti-money laundering and combating the financing of terrorism (AML/CFT) requirements *"are not the core Central Bank objective and will not be the primary motivation to issue a CBDC"* (BIS 2020, 6), whereas for the Bank of Canada, *"privacy is not the sole purview"* (Shah et al. 2020). They also comment that they needed to determine the precise level of privacy by consulting with external institutions (e.g., law enforcement, financial transactions, and reports, etc.). The Reserve Bank of New Zealand noted that *"its proposed retail CBDC would balance privacy protection and the government's traceability requirement to reduce tax evasion, avoidance, money laundering, and terrorism financing"* (Kshetri and Loukaianova 2022, 97).

Even though CBDC will likely hinder direct criminal use, criminals will still want to acquire it, as it will be broadly adopted by merchants and possess some novel technical features such as micropayments and programmability (Fanusie 2020). As a result, financial authorities should be aware of illicit actors trying to get dirty money into the CBDC system. Illicit actors will likely adapt the rollout of a CBDC by developing more sophisticated money laundering schemes that trade cash and anonymous digital tokens for CBDC (ibid). Darbha and Rakesh (2020) outline that the main concern of privacy in a CBDC is what information to keep private and from whom, as many people see privacy differently. Nevertheless, they illustrate what is technically feasible for Central Banks, such as choosing cryptographic techniques and operational arrangements that have an in-built privacy design.

Another technical proposal is a token based CBDC that combines transaction privacy with KYC and AML/CFT compliance, as well as blind signatures (Grothoff and Moser 2021). Technology offers many degrees of flexibility in deciding and implementing privacy and anonymity options. As an example, privacy may be assured for offline transactions below a

certain threshold (Brunnermeier and Landau 2022). In the framework of most countries, privacy is recognized for transactions up to a certain amount. When significant amounts of cash are exchanged, they must be declared. (In Europe, cash transactions exceeding 10,000 EUR must be reported: ER 2018). For example, China's Central Bank announced that consumers with less than 10,000 yuan and daily transactions of less than 2000 and 5000 yuan are simply identifiable by their mobile phone subscribers that are regulated by telecom operators. Only above the threshold would ID and banking information be required. As a result, transactions would be accessible for financial intermediaries and authorities in charge of AML/CFT regulations (PBoC 2021). However, Dupuis, Gleason, and Wang (2022) point out that certain nations, like China, presently exhibit low scores in terms of personal freedom, raising questions about the tradeoffs between AML rules and privacy rights.

In Sweden's approach, according to Riksbank (2021), e-krona would most likely meet AML and CTF requirements. All businesses that provide electronic payment and payment services must comply with the Swedish legislation on measures against AML and CFT. The Riksbank would provide e-krona to network participants, and participants, who might be commercial banks, would transfer e-krona to the end users. As a result, the members of the e-krona network would be responsible for KYC. The KCY and monitoring of transactions would remain within the distributors, as it is currently the case. This implies that participants, such as commercial banks, are required to know who their customers are that utilize payment systems (KYC). They also indicate that e-payments would leave traces and that the Riksbank and its intermediaries would investigate any illicit use of e-krona. Beyond that, they argue that there is a tradeoff between privacy and resilience, with greater privacy resulting in less resilience. Anonymous payments and smaller sums would be permitted, but only to a limited degree according to existing AML legislation. Riksbank (2021, 14) claims that anonymous e-kronor may exist, but only in a "very limited area of use".

Furthermore, the ECB has proposed allowing so-called "anonymity vouchers" for a specific number of private transactions in the digital euro (ECB 2019). These vouchers would allow users to transfer a specified or limited amount of CBDC anonymously over a period. In addition, neither Central Banks nor counterparties could view transaction histories, only the user. Hence, individuals would have control over a limited number, thereby protecting privacy.

6.5. Evaluation of Interview results and analysis

First, it should be noted that the experts represent specialist areas, and in the case of other specialized topics, the experts lacked the relevant expertise to provide the appropriate answer. Hence, in some cases, the experts refrained from answering individual questions.

To begin with, the experts are questioned in Q1 to discuss major challenges and drawbacks a CBDC has with respect to privacy. E1 shared that: *"Privacy is kind of a two-edged sword for Central Banks in the hemisphere. On the one hand, you don't want to seem like a giant sponge soaking up the citizens' data (which would lead to reluctance to adopt the CBDC in some jurisdictions like Germany). On the other hand, you must fulfill AML/CFT regulations, because you don't want your CBDC to be a safe haven for illicit activities*". However, E2 stated that *"the only drawback results in traceability, which must be undermined to solve privacy issues."* Furthermore, E2 added that the main objective is to have characteristics of a *"cash-like design, and that depends on the technical design of a CBDC".* From a practical perspective, the results of the evaluation of Q1 reveal that the experts generally see the biggest challenge in tracking the data in a Central Bank coin, which is also consistent with the literature findings from chapter 3, among other things.

In Q2, five experts responded with an average value of 1.3 on a scale from 1 to 5, reaching almost the minimum value for this parameter and suggesting that spamming, stalking, etc., do not occur when a CBDC is designed to lack privacy. In contrast to the scholarly view, experts do not consider problems such as spamming, being stalked, or having your identity stolen to be relevant. Instead, the lack of privacy is caused by stricter control and monitoring

by Central Banks or governments. This is also evident in the following statement by E3: *"These are not problems with lack of privacy; lack of privacy would rather enable Central Banks, etc., to gather and process the data. As a result, the individual, the data subject would be subject to stricter control and supervision."*

In Q3, the experts are asked to determine whether a CBDC can provide the same privacy as cash and what the privacy benefits of a CBDC are. As stated in Chapter 1, cash is anonymous, and a CBDC will always leave electronic traces. The experts strongly agree with this statement and shared that a CBDC is indistinguishable from cash; E5 stated a CBDC "*will always lose; even if the CBDC were to be totally anonymous, you would still have digital traces. It is crucial to design it from the beginning with privacy in mind, as it cannot be added later."*

Drawing on the previous question, the experts were asked in Q4 whether it is feasible to design a CBDC in such a way as to make it untraceable. The literature suggests that most Central Banks do not aim to operate in untraceable way, but the technical design could be a means to do so and still meet both objectives. Despite that, the views of the experts are somewhat varied. E1 answered, *"No, because then we could not follow current AML/CFT and KYC regulations."* While E2 and E3 consider that it can be designed untraceable and highlight towards technical capabilities, such as blind signatures and DLT technology, respectively. E5 noted *that "there are some technical options that are potential solutions, but it is still necessary to address this issue, as currently there are only options and no solutions based on them yet."*

Furthermore, experts are asked in Q5 to give their views on whether a CBDC could be more trustworthy with legal entrenchment, meaning enriched in law as legal tender, as in the example of China's e-CYN. As mentioned in Chapter 1, cash is the sole type of legal tender that Central Banks provide, and the question whether a CBDC should have a legal tender status is widely debated. On the one hand, most experts believe that it should have legal tender status in order to be accepted by consumers in the first place and to gain trust in digital currency. But

opinions remain ambivalent, which is consistent with the literature. This is also reflected in E3's statement: "*A legal entrenchment won't hurt, but the positive effect would be minor.* According to E3 research, *most people are not aware of the concept and don't know that digital money is not created by Central Banks. As a result, people who distrust CBDC will also likely distrust political, legal or governmental institutions".*

Next, in Q6, the experts are asked what other safeguards (e.g., fundamental rights, data protection) exist for privacy in a CBDC. It can be said that the E1, E3 and E5's opinion coincides with the codified laws expressed in the literature (CFR 2007; ECtHR 1950; UNGA 1948; EP 2016) and that the most important safeguards are declared to be fundamental rights. On the other side, E4 expressed that: "*These, however, do not guarantee that these rights are not violated; other safeguards would be continuous supervision of the enforcement of this regulation; that also means that a CBDC should be designed from the beginning in such a way that all actors are not able to gather information and inferences from CBDC transaction data to perform activities against their wishes."* E1 referred to the existing data protection regulation, followed by technical design (pseudonymity, cyber resilience).

The second part of the interview guide focuses on solutions to protect privacy while uncovering IFA. The literature confirms that different approaches and choices are dependent on the objectives of the respective jurisdiction. Since most projects are still in development, the decisions may not be final.

In Q7, the experts are asked about the capabilities to ensure as much privacy as possible while still detecting IFA. Three experts answered the question. E3 stated that "*research is lacking in this regard,"* whereas E1 noted, *"to make use of existing intermediaries and use their known capabilities of fighting financial crime"* E5 expressed that *"this is a crucial thing because both data and privacy can be abused. One way is to have asymmetric privacy, meaning that you have total anonymity as the payer but not as the receiver. So, the receiver cannot, e.g.,*

avoid taxes. The tricky thing is that it is different from what is required by the regulator, and this is an area where you clearly see that governments would like to have more information". In questions 8, 9, and 10, the experts are asked three assertions about potential solutions concerning privacy and illicit financial activity.

First, in Q8 the experts were asked whether technical design (e.g., cryptographic techniques, token-based, etc.) could be a solution. As assessed in Chapter 3, the literature suggests that there are technical options to solve the problem. This is also in line with the expert's findings, as they rate an average value of 4,3 on a scale from 1 to 5, which generally indicates that experts consider technical design as a potential solution. Nonetheless, some experts have also acknowledged the negative aspects of technical design choices. E3 pointed toward the fact that *"more research is needed here; there might be many options and advances for privacy, but the implementation is the challenging part. In addition, these also come with other disadvantages,"* while E4 stated that*: "Technological innovation can be a means to balance these competing priorities, but technology is simply inadequate to avoid the misuse of this data if the government insists on the data."*

In Q9, the experts are asked if legislation (e.g., changing the law) could help. It is to be noted that this question goes beyond what is presented in the literature. However, E1 notes that *"regulation can only create the prerequisites for solving crime, but the main weight falls on the investigative authorities."* On the contrary, E4 expressed: *"The assumption is that CBDC must comply with all these existing AML, CFT, and KYC rules, but this is not necessarily true. The regulations are statutory, but Congress could modify these obligations. There should be a more informed discussion of how privacy in CBDC should be preserved at the legal level, rather than solely relying on technology that might not have been tested in real-life scenarios."*

Q10 yields an average score of 3,33 on a scale from 1 to 5 after being asked whether threshold or anonymity vouchers could solve the problem. It should be noted that this falls

partially into the category of technological capabilities. As elaborated in the literature, for some countries, these design options might be a feasible option to safeguard privacy but also help detect IFA. While most experts rated between 3 and 5 of a scale from 1 to 5, E2 rated 1 and argued: "*Threshold/ Anonymity vouchers cannot improve privacy because privacy is obtained by their design."* E1 also mentioned being aware of techniques such as *"smurfing".* Furthermore, E3 stated that *"most Central Banks will decide against it because it appears unconventional and messy."*

Last, the experts are asked what other potential options there might be to safeguard privacy but detect IFA. Four experts expressed their views on this: E1 stated that *"self-sovereign identities could come in handy..."* E2 outlined that "*zero-knowledge proofs and the encoding of identity in coins would be another way to protect the privacy and detect illegal financial activity…but illegal financial activities will always find their way, just like in today's world. Measures will not be sufficient to fully detect IFA.*" E4 further argues *"that regular audits of government access to private transactions could be performed by an independent body explicitly designed to protect user privacy, which in turn could also monitor for potential AML/ CTF abuse."* On the other side, E5 argued that *"usually you have some parliamentary committee to monitor the government, but the experience is that it doesn't really work well. Another option would be to distribute keys, so to get access to that data, you need both the government and the user to agree, and only with both keys can you access data or white papers. I have faith in the technical solutions, but they must be tested further."*

In conclusion, neither a review of scholarly perspectives nor data gathered from the experts have confirmed a unified perception of how to protect privacy while facilitating IFA activity. There is no universal view on the design of a CBDC, as it largely depends on the different objectives and technological design options, as well as the legal framework.

6.6. Conclusion

This chapter has primarily contributed to a better understanding of privacy and IFA and carefully studied potential solutions to safeguard privacy issues and IFA, along with existing scholarly research and the opinions of experts in the field. Privacy and IFA go hand in hand and are both integral components of the design of a CBDC. There are many complex considerations surrounding which authorities will have the data, how they can use it, and under what circumstances. Payments give insights into individuals behavior, and a CBDC could make individuals prone for being used for political purposes, for example. Privacy in CBDC cannot be compared to privacy in cash, as there will always be digital traces. It can be said that there is no one-size-fits-all CBDC solution that would be suitable for all Central Banks, as the design is dependent on the diverse policy objectives of each jurisdiction.

The chapter outlines modern design options, including cryptographic techniques such as limits or anonymity vouchers, etc., that can mask identity. The experts, as well as the scholars view technical design as a potential solution, despite one group of experts in the study also sharing technical concerns and found the topic to be controversial. These choices would not hinder the misuse of data, and research on the topic is lacking, as all these options merely provide a technical framework and are not yet final. Furthermore, the chapter has concluded additional methods to safeguard privacy and detect IFA. The experts interviewed outlined self-sovereign identities, zero-knowledge proofs, encoding of identities, blind signatures, etc. as potential methods from the technical side. These possible solutions could offer higher degrees of privacy and IFA protection, but they would require further testing based on real-life situations, as most banks are still in the research phase. Additionally, one expert emphasized doing regular audits by an independent body, while another noted that there should be a more informed discussion about how privacy can be ensured at the legal level, as technology is continuously evolving along with unanticipated challenges. Technical frameworks cannot be made effectively without the backbone of an effective legal regulatory framework.

Chapter 7: Conclusion and final remarks – Group part

Current CBDC research has only partially addressed the implications and challenges of launching a retail CBDC on various stakeholders such as Central Banks, commercial banks, and end-users. Therefore, we believe that this thesis contributes to fill a research gap, by analyzing the key implications and challenges of a general-purpose CBDC from three different perspectives: economics, privacy, and technology. This holistic approach allowed us to understand the global impact of CBDCs, apart from the various trade-offs that exist.

We contribute to the existing literature by conducting interviews with experts from various industries to provide superior recommendations for retail CBDC designers on how to successfully develop digital currency to mitigate legal and financial risk. We realized that implementing a new form of alternative payment for the public will have a significant effect on the economy and society. Therefore, Central Banks are strongly recommended to conduct a full-scale analysis and several pilot projects before integrating CBDC as a new means of payment. This involves inter alia the preparation of a strategic roadmap with clear objectives that are aligned with domestic policy, legal and financial foundational principles. Furthermore, it is essential to link the architectural model with country-specific legal, financial, and cultural frameworks, since a universal approach would not be the most viable option due to strong discrepancies. In addition, an extension of the domestic r-CBDC model is imperative to ensure international operability with digital currencies of other countries.

Due to the strong impact on different stakeholders, it is crucial that CBDCs are successful if implemented, mainly in terms of acceptance, convenience, and resilience of payment systems. In fact, if CBDCs are not widely adopted due to complexity or even safety issues, this could raise a variety of questions on Central Bank's authority and reliability. The truth is that one of the main motivations of Central Banks to launch a CBDC relies on the current digital and cryptocurrency trends observed in the markets, which may undermine Central Banks' authority and monetary sovereignty. In fact, if adopted widely, private digital

currencies might hinder the effectiveness of monetary policy and even financial stability. Even if valid, this reason alone does not seem to be enough for the creation of CBDCs, as this should be an innovation moved not only by a Central Bank need, but also by public/end-user need.

The three different analyses allowed us to gather a broad range of opinions, ranging from scholars to experts working in different industries. Starting with Chapter 4, one can mention the importance of aligning CBDCs with the financial stability goal of Central Banks, given that a CBDC that would harm one of the main goals of Central Banks would be counterproductive and even lose its purpose. Depending on the design, CBDCs might heavily change the landscape under which monetary policy is conducted. On the one hand, they may eliminate the need for unconventional policies, given the ability to perfection the monetary policy transmission mechanism through an interest bearing CBDC. On the other hand, unconventional policies such as Helicopter Money might be easier to conduct, given the enhanced targeting capacity of Central Banks when injecting funds in the economy. Plus, the CBDC design will necessarily influence the higher or lower risk of bank runs and bank disintermediation, thereby influencing financial stability in a positive or negative way.

Chapter 5 analyzed the various design considerations and the associated trade-offs that the CBDC designer might face when implementing a retail CBDC for the general public. It is suggested that each Central Bank select the most appropriate design choice with professional judgement and align it with domestic cultural, legal and policy objectives. The pursuit of a collaborative design approach with other stakeholders minimizes the risk of developing a digital currency with low viability. The two common key factors that should be on the priority list of each CBDC designer are "*Privacy*" and "*Interoperability*". Additionally, recent technologies provide myriad opportunities to make payment systems more cost efficient (e.g., reduction in cost of currency management), however, there are some critical touchpoints that need to be considered by CBDC practitioners to mitigate the threat of bad actors committing cyber- and

sophisticated malicious attacks. Therefore, appropriate measures need to be developed to leverage the benefits of the respective CBDC system. Lastly, significant importance needs to be place on the societal education about r-CBDC merits to ensure a high adoption.

Chapter 6 examined the implications and challenges of privacy in a CBDC with respect to IFA. Both components are integral in the design of a CBDC and must be balanced to preserve privacy of CBDC users and protect their data while combating illegal activity. The study identifies several technical design options, that cannot be made effectively without the backbone of a legal regulatory framework. These technological options need further testing based on real-world cases, as most banks are still in the pilot and research phase. It is to be noted that the design of a CBDC depends on the objectives of the respective jurisdiction and must therefore provide regulatory clarity as a preliminary objective.

7.1 Limitations and Future research

CBDCs are currently on the verge of being introduced by many Central Banks worldwide, and yet there are many unanswered questions. Once implemented, it would be relevant to assess the financial and economic impact of CBDCs in different geographies and jurisdictions, by having real-life numbers on the acceptance, use and on the implications on both Central Banks and commercial banks' balance sheets. This would allow to examine country-specific and regional case studies on the design of CBDCs. Also, the "financial inclusion" argument should be further investigated to confirm or deny that underdeveloped economies will benefit from CBDCs.

In addition, there are still questions related to the environmental impact of CBDCs, mainly the energy consumption aspect which should be investigated in the future. Plus, setting a holding rate or limit on CBDC deposits can reduce its attractiveness compared to cash. Thus, this balance on user preferences should be addressed in the future. Once empirical evidence is gathered, it will be revealed if CBDCs, as a disruptive innovation, can deliver on the promises made in the literature and by supporters.

References

Adalid, Ramón, Álvaro Álvarez-Blázquez, Katrin Assenmacher, Lorenzo Burlon, Maria Dimou, Carolina López-Quiles, Natalia Martín Fuentes, et al. 2021. "Occasional Paper Series Central Bank Digital Currency and Bank Intermediation Exploring Different Approaches for Assessing the Effects of a Digital Euro on Euro Area Banks."

Adleman, L., R. L. Rivest, and A. Shamir. 1978. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems."

Adrian, Tobias, and Mancini-Griffoli Tommaso. 2019. "The Rise of Digital Money." Washington: International Monetary Fund.

Agarwal, Ruchir, and Miles Kimball. 2015. *Breaking Through the Zero Lower Bound*. International Monetary Fund Working Paper 15/224.

Agrawal, Shikha, and Ruchi Verma. 2013. "Data Security for Any Organization by Using Public Key Infrastructure Components and MD5, RSA Algorithms." IJRET: International Journal of Research in Engineering and Technology, 819–25.

Aguirre, Illich, John Arroyo, Bobby Chen, Mario Griffiths, Gabriela Guiborg, Natalie Haynes, Allister Hodge, et al. 2021. "Implementing a Retail CBDC: Lessons Learned and Key Insights." Latin American Journal of Central Banking 2 (1): 100022. https://doi.org/10.1016/j.latcb.2021.100022.

Agung, Anak Agung Gde, Rixard George Dillak, Robbi Hendriyanto, and Devie Ryana Suchendra. 2019. "Proof of Work: Energy Inefficiency and Profitability." Article in Journal of Theoretical and Applied Information Technology 97 (5): 1623–33.

Agur, Itai, Anil Ari, and Giovanni Dell Ariccia. 2020. "Designing Central Bank Digital Currencies." Journal of Monetary Economics. Vol. 125. Elsevier B.V.

Agur, Itai, Anil Ari, Fabio Comelli, Tommaso Mancini Griffoli, Federico Grinberg, Ashraf Khan, John Kiff, et al. 2018. Casting Light on Central Bank Digital Currency. International Monetary Fund.

Ajayi, S Ibi. 1999. "Evolution and Functions of Central Banks." Vol. 37.

Al-Ahmad, Ahmad, Yehia Ibrahim Alzoubi, Ashraf Jaradat, and Hasan Kahtan. 2022. "Internet of Things and Blockchain Integration: Security, Privacy, Technical, and Design Challenges." Future Internet 14 (7): 1–48.

Allen, Franklin, Xian Gu, and Julapa Jagtiani. 2022. "Fintech, Cryptocurrencies, and CBDC: Financial Structural Transformation in China." *Journal of International Money and Finance 124.*

Allen, Michaella, Barry Cooper, and Antonia Esser. 2019. "The Use Cases of Central Bank Digital Currency for Financial Inclusion: A Case for Mobile Money."

Allen, Sarah, Srđjan Čapkun, Ittay Eyal, Giulia Fanti, Bryan A Ford, James Grimmelmann, Ari Juels. 2020. “Design Choices for Central Bank Digital Currency: Policy and Technical Considerations.” National Bureau of Economic Research.

Alliance for Financial Inclusion. 2022. “Central Bank Digital Currency- An Opportunity for Financial Inclusion in Developing and Emerging Economies.” Malaysia.

Altavilla, Carlo, Lorenzo Burlon, Mariassunta Giannetti, and Sarah Holton. 2019. “Working Paper Series Is There a Zero Lower Bound? The Effects of Negative Policy Rates on Banks and Firms.”

Alwazir, Jihad, Charles Kahn, and Manmohan Singh. 2022. “Digital Money and Central Bank Operations, WP/22/85, May 2022.”

Andesta, Erfan, Fathiyeh Faghih, and Mahdi Fooladgar. 2019. “Testing Smart Contracts Gets Smarter,” December.

Antonopoulos, Andreas M. 2014. Mastering Bitcoin : Unlocking Digital Cryptocurrencies. Edited by Mike Loukides and Allyson MacDonald. First Edition. Sebastopol: O’Reilly Media.

Armelius, Hanna, Paola Boel, Carl Andreas Claussen, and Marianne Nessén. 2018. “The E-Krona and the Macroeconomy.”

Ashford, Nicholas A., Ralph P. Hall, and Peter Söderbaum. 2008. “Trade-off Analysis as an Alternative to Cost-Benefit Analysis in Socio-Technical Decisions.” Oslo.

Assenmacher, Katrin, and Signe Krogstrup. 2021. “Monetary Policy with Negative Interest Rates: De-Linking Cash from Digital Money.” International Journal of Central Banking 03 (67): 67–106.

Aste, Tomaso, Antonio Briola, David Vidal-Tomás, and Yuanrong Wang. 2022. “Anatomy of a Stablecoin’s Failure: The Terra-Luna Case.” Finance Research Letters, September, 103358.

Atlantic Council (AC). 2022. “CBDC Tracker”.

Attanasio, Silvia, Teana Baker-Taylor, Burkhard Balz, Stefan Berger, Jan Ceyssens, Eric Demuth, Michael Gronager, et al. 2022. “Digital Euro Summit.” November 15, 2022.

Auer, Raphael, and Rainer Böhme. 2021. “Central Bank Digital Currency: The Quest for Minimally Invasive Technology.” www.bis.org.

Auer, Raphael, Giulio Cornelli, and Jon Frost. 2020. “Rise of the Central Bank Digital Currencies: Drivers, Approaches and Technologies.” CEPR Discussion Paper No. DP15363.

Auer, Raphael, Philipp Haene, and Henry Holden. 2021. “Multi-CBDC Arrangements and the Future of Cross-Border Payments.”

Aysan, Ahmet and Farrukh Kayani. 2022. *"China's transition to a digital currency does it threaten dollarization."* Asia and Global Economy 2 (100023).

Azmathullah, Rahima Meer, Faiza Rizwan, and Husneara Sheikh. 2018. "Proof-of-Work vs Proof-of-Stake: A Comparative Analysis and an Approach to Blockchain Consensus Mechanism." International Journal for Research in Applied Science & Engineering Technology (IJRASET) 6 (XII): 2321–9653.

Baeriswyl, Romain, Samuel Reynard, and Alexandre Swoboda. 2021. "Retail CBDC Purposes and Risk Transfers to the Central Bank." 19. Zurich.

Bakas, Dimitrios, Magkonis Georgios, Oh Eun Young. 2022. "What drives volatility in Bitcoin market?" *Finance Research Letters 50.*

Ballaschk, David, and Paulick Jan. 2021. "The Public, the Private and the Secret: Thoughts on Privacy in Central Bank Digital Currencies." *Journal of Payments Strategy & Systems. Vol. 15.*

Banisar, David. 2006. "Freedom of Information Around the World 2006." A Global Survey of Access to Government Information Laws.

Bank for International Settlements. 2021. "III. CBDCs: An Opportunity for the Monetary System."

Bank of Australia, Reserve. 2020. "Bulletin September Quarter 2020."

Bank of England. 2020. "Central Bank Digital Currency Opportunities, Challenges and Design."

Bank Of International Settlements (BIS). 2018. "Central Bank Digital Currencies." CPMI, Markets Committee Paper, No 174.

Bank of International Settlements (BIS). 2020. "Central Bank Digital Currencies: Foundational Principles and Core Features." BIS Innovation Hub, Report No. 1

Barrdear, John, and Michael Kumhof. 2016. "Staff Working Paper No. 605 The Macroeconomics of Central Bank Issued Digital Currencies."

Basel Committee on Banking Supervision. 1997. "Core Principles for Effective Banking Supervision."

Baur, Dirk G., and Lai T. Hoang. 2021. "A Crypto Safe Haven against Bitcoin." Finance Research Letters 38 (January).

Bech, Morten, and Rodney Garratt. 2017. "Central Bank Cryptocurrencies 1." BIS Quarterly Review. Basel. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3041906.

Bech, Morten, Codruta Boar, Claudio Borio, Stijn Claessens, Benoît Coeuré, Jon Frost, Leonardo Gambacorta. 2020. "The Technology of Retail Central Bank Digital Currency." BIS Quarterly Review.

Bechara, Marianne, Wouter Bossu, Natasha Che, Sonja Davidovic, Tommaso Mancini Griffoli, John Kiff, Inutu Lukonga, Gabriel Soderberg, Tao Sun, and Akihiro Yoshinaga. 2022. Behind the Scenes of Central Bank Digital Currency Emerging Trends, Insights, and Policy Lessons. Edited by Erica Sandoval. Washington: International Monetary Fund.

Bechtel, Alexander, Jonas Gross, Philipp Sandner, and Victor von Wachter. 2020. "Programmable Money and Programmable Payments."

Bedford, James, Stuart Berry, Kalin Nikolov, and Chris Young. 2009. "Quantitative Easing."

Belke, Angar, Daniel Gros, and Thomas Osowski. 2017. "The Effectiveness of the Fed's Quantitative Easing Policy: New Evidence Based on International Interest Rate Differentials." *Journal of International Money and Finance* 73 (May): 335–49.

Bell, Emma and Bryman Alan. 2006. "The Ethics of Management Research: An Exploratory Content Analysis". British Journal of Management, Volume 18, Issue 1.

Bender, Marc, Caroline Bennet, Reginia Chan, Grant Frear, Eng Hong Lim, Mohit Mehrotra, Tim Pagett, Monish Shah, and Shweta Shetty. 2022. Central Bank Digital Currencies: Building Block of the Future of Value Transfer.

Benigno, Gianluca, and Pierpaolo Benigno. 2022. "Managing Monetary Policy Normalization."

Bennet, Caroline, Reginia Chan, Monish Shah, and Shweta Shetty. 2022. "Central Bank Digital Currencies: Building Block of the Future of Value Transfer."

Berger, Wolfram, and Friedrich Kißmer. 2013. "Central Bank Independence and Financial Stability: A Tale of Perfect Harmony?" European Journal of Political Economy 31 (September): 109–18.

Bernanke, Ben. 2016. "What Tools Does the Fed Have Left? Part 3: Helicopter Money." *Brookings*, April.

Bindseil, Ulrich, and Alessio Fotia. 2021. "Introduction to Central Banking."

Bindseil, Ulrich, Fabio Panetta, and Ignacio Terol. 2021. "Central Bank Digital Currency: Functional Scope, Pricing and Controls." 286. Frankfurt. https://doi.org/10.2866/970879.

Bindseil, Ulrich. 2019. "Central Bank Digital Currency: Financial System Implications and Control." *International Journal of Political Economy* 48 (4): 303–35.

Bindseil, Ulrich. 2020. "Tiered CBDC and the Financial System." 2351. Frankfurt.

BIS, CPMI, IMF, and World Bank Group. 2022. "Options for Access to and Interoperability of CBDCs for Cross-Border Payments."

Bitter, Lea. 2020. "Banking Crises under a Central Bank Digital Currency (CBDC)."

Böhme, Rainer, Auer Raphael, Clark Jeremy, Didem Demirag. 2022. "Mapping the Privacy Landsscape for Central Bank Digital Currencies". Acmqueue, Volume 20, issue 4.

Boissay, Frederic, Giulio Cornelli, Sebastian Doerr, and Jon Frost. 2022. “Blockchain Scalability and the Fragmentation of Crypto.” 56. www.bis.org.

Bonis, Riccardo de, and Giuseppe Ferrero. 2022. “Technological Progress and Institutional Adaptations: The Case of the Central Bank Digital Currency (CBDC).” 690. Rome.

Bordo, Michael D, and Andrew T Levin. 2017. “NBER WORKING PAPER SERIES CENTRAL BANK DIGITAL CURRENCY AND THE FUTURE OF MONETARY POLICY.”

Borio, Claudio, Stijn Claessens, Benjamin Cohen, Dietrich Domanski, Hana Halaburda, Krista Hughes, Jochen Schanz, Hyun Song, Morten Bech, and Rodney Garratt. 2017. “Central Bank Cryptocurrencies 1.” BIS Quarterly Review.

Boston Consulting Group (BCG). 2018. “Briding the trust gap in personal data”.

Bourreau, Marc. 2017. “Data and Competition Policy: Market Power, Personalised Pricing and Advertising Project Report.” Centre on Regulation in Europe (CERRE).

Britannica, T. Editors of Encyclopaedia. 2019. "central bank." *Encyclopedia Britannica*, July 24, 2019.

Brokke, Olav, and Nils-Eirk Engen. 2019. “Central Bank Digital Currency (CBDC) An Explorative Study on Its Impact and Implications for Monetary Policy and the Banking Sector.”

Brousmiche, Kei Leo, Elyes ben Hamida, Hugo Levard, and Eric Thea. 2017. “Blockchain for Enterprise: Overview, Opportunities and Challenges.” In , 1–7. Nice, France : The Thirteenth International Conference on Wireless andMobile Communications (ICWMC 2017)

Brousmiche, Kei-Leo, Omar Dib, Antoine Durand, Ben Hamida, and Eric Thea. 2018. “Consortium Blockchains: Overview, Applications and Challenges.” International Journal on Advances in Telecommunications 11 (1–2): 51–64. http://www.iariajournals.org/telecommunications/.

Browne, Ryan. 2022. “Christine Lagarde Says Crypto Is Worth Nothing.” CNBC, May 23, 2022.

Brunnermeier, Markus and Landau Jean-Pierre. 2022. “The Digital Euro: Policy Implications and Perspectives.” Suerf – The European Money and Finance Forum.

Buchholz, Katharina. 2022. “China’s Mobile Payment Adoption Beats All Others,” July 8, 2022.

Bukele, Nayib. 2021. Why El Salvador Made Bitcoin Legal Tender with President Nayib Bukele.

Capkun, Srdjan, Arthur Gervais, Vasileios Glykantzis, Ghassan O Karame, Hubert Ritzdorf, and Karl Wüst. 2022. “On the Security and Performance of Proof of Work Blockchains.”

Castillo-Montoya, M. 2016. *"Preparing for Interview Research: The Interview Protocol Refinement Framework."* The Qualitative Report, 21 (5), 811-831.

CBDC Global Index, PWC. 2021. "Central Bank Digital Currencies (CBDC) Index Report."

CBDC Tracker. 2022. "Today's Central Bank Digital Currencies Status." CBDC Tracker . December 8, 2022. https://cbdctracker.org/.

Central Bank Bahamas. 2019. *Project Sand Dollar: A Bahamas Payments System Modernisation Initiative*.

Central Bank Nigeria. 2021. *Design Paper for the eNAIRA.*

Central Bank. 2020. *Report on a digital euro*.

Chakravarty, Manuel M.T., James Chapman, Kenneth MacKenzie, Orestis Melkonian, Michael Peyton Jones, and Philip Wadler. 2020. The Extended UTXO Model. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Vol. 12063 LNCS. Springer.

Chao, Fei, Li Honglei, Yang Longzhi, Naik Nitin, and Elisa Noe. 2019. "Consortium Blockchain for Security and Privacy-Preserving in E-Government Systems." In Proceedings of The 19th International Conference on Electronic Business , 99–107. Newcastle upon Tyne, UK: ICEB.

Charter of the Fundamental Rights. 2017. "Article 8 – Protection of personal data." Official Journal of the European Union C303/17.

Che, Natasha, Ankita Goel, Sarwat Jahan, Mike Li, Elena Loukoianova, Evan Papageorgiou, Umang Rawat, and Sarah Yong Zhou. 2022. Towards Central Bank Digital Currencies in Asia and the Pacific.

Chen, Hongyi, and Pierre L. Siklos. 2022. "Central Bank Digital Currency: A Review and Some Macro-Financial Implications." *Journal of Financial Stability* 60 (June).

Chen, Xiangping, Hong Ning Dai, Huaimin Wang, Shaoan Xie, and Zibin Zheng. 2018. "Blockchain Challenges and Opportunities: A Survey." International Journal of Web and Grid Services 14 (4): 352–75.

Cheng, Pangyue. 2022. "Decoding the rise of Central Bank Digital Currency in China: design problems, and prospects". Journal of Natural Public Health Emergency Collection.

Chohan, Usman W. 2022. "Central Bank Digital Currencies (CBDCs)."

Chorzempa, Martin. 2021. "Promise and Peril of Digtal Money in China." Cato Journal.

Choulet, Céline, and Yelena Shulyatyeva. 2016. "History and Major Causes of US Banking Disintermediation."

Cœuré, Benoît 1969-, Jon Cunliffe, Bank für Internationalen Zahlungsausgleich, Bank of Canada, Europäische Zentralbank, Nihon Ginkō, Sveriges Riksbank, Schweizerische Nationalbank, Bank of England, and Federal Reserve System Board of Governors. 2020.

Central Bank Digital Currencies: Foundational Principles and Core Features Report No. 1 in a Series of Collaborations from a Group of Central Banks.

Coeuré, Benoît, and Hyun Song Shin. 2021. "CBDCs: An Opportunity for the Monetary System." Basel.

Cœuré, Benoit, and Jacqueline Loh. 2018. "Central Bank Digital Currencies." 174. Basel. www.bis.org.

Counsell, Steve, Natalia Dashkevich, and Giuseppe Destefanis. 2020. "Blockchain Application for Central Banks: A Systematic Mapping Study." IEEE Access 8: 139918–52.

D'ippoliti, Carlo, Lucio Gobbi, and Jacopo Temperini. 2022. "Is the Time Ripe for Helicopter Money? Growth Impact and Financial Stability Risks of Outright Monetary Transfers *."

Darbha, Sriram and Rakesh Arora. 2020. "Privacy in CBDC technology." Staff Analytical Note 2020 – 9, Bank of Canada.

Dark, Cameron, Tony Richards, and Chris Thompson. 2020. "Retail Central Bank Digital Currency: Design Considerations, Rationales and Implications." Sydney.

Davoodalhosseini, Mohammad, Francisco Rivadeneyra, and Yu Zhu. 2020. "CBDC and Monetary Policy." 2020–4.

Deng, J. 2020. "*The impact of Central Bank digital currencies on third-party payments."* Modern Bankers.

Dlodlo, Nomusa, Tyron Ncube, and Alfredo Terzoli. 2020. "Private Blockchain Networks: A Solution for Data Privacy." In 2020 2nd International Multidisciplinary Information Technology and Engineering Conference, IMITEC 2020, 2–9. Institute of Electrical and Electronics Engineers Inc.

Dupuis, Daniel, Kimberly Gleason, and Zhijie Wang. 2022. "Money Laundering in a CBDC World: A Game of Cats and Mice." Journal of Financial Crime 29 (1): 171–84.

Dyson, Ben, and Graham Hodgson. 2016. "Why Central Banks Should Start Issuing Electronic Money DIGITAL CASH Download Permission to Share."

Eichengreen, Barry, and Yong Xia. 2022. "Central Bank Digital Currencies: Implementation, Applications and Challenges." In . HKUST Business School.

Engert, Walter, and Ben Siu-Cheong Fung. 2017. "Central Bank Digital Currency: Motivations and Implications."

Entrop, Oliver, Christoph Memmel, Benedikt Ruprecht, and Marco Wilkens. 2015. "Determinants of Bank Interest Margins: Impact of Maturity Transformation." *Journal of Banking and Finance* 54: 1–19.

EU Blockchain. 2022. "Decentralised Finance (DeFi)."

European Central Bank (ECB). 2019. "Exploring Anonymity in Central Bank Digital Currencies."

European Central Bank (ECB). 2021. “Eurosystem report on the public consultation on a digital euro.”

European Central Bank. 2019. “What Is a Lender of Last Resort?” August 26, 2019.

European Comission. 2010. “COMMISSION RECOMMENDATION of 22 March 2010 on the Scope and Effects of Legal Tender of Euro Banknotes and Coins (2010/191/EU).”

European Commission (EC). 2021. “Beating Financial Crime: Commission Overhauls Anti-Money Laundering and Countering the Financing of Terrorism Rules.” Press Release.

European Commission. 2022. “Crypto-Asset Markets,” July 26, 2022.

European Court of Human Rights. 1950. “European convention of human rights.” European Treaty Series – No. 5.

European Data Protection Supervisor. 2022. “Data Protection.” 2022.

European Parliament and Council of the European Union (EP and EUCO) . 2016. “General Data Protection Regulation (GDPR). *Official Journal of the European Union. L119, p. 1-88*

European Regulation (ER). 2018. “Regulation (EU) 2018/1672 of the European Parliament and of the Council (4).” Offical Journal of the European Union.

Fanti, Giulia, and Nadia Pocher. 2022. “Privacy in Cross-Border Digital Currency: A Transatlantic Approach.” http://www.jstor.org/stable/resrep43397.

Fanti, Giulia, Leonid Kogan, and Pramod Viswanath. 2019. “Economics of Proof-of-Stake Payment Systems.”

Fanusie, Yaya J. 2020. “Central Bank Digital Currencies: The Threat from Money Laundering and how to stop them.” The Digital Social Contract: A Lawfare Paper Series.

Federal Reserve (FED). 2022. “Federal Reserve Discussion Paper on Central Bank Digital Currency Paper Outlines ‘Pros and Cons’ of a CBDC”.

Federal Reserve System. 2018. “Principles for the Conduct of Monetary Policy.” 2018.

Ferguson, John and Shannon Parker. 2020. “Perspectives on Chinese Digital RMB Strategy.”

Fernández-Villaverde, Jesús, Daniel Sanches, Linda Schilling, and Harald Uhlig. 2021. “Central Bank Digital Currency: Central Banking for All?” *Review of Economic Dynamics* 41 (July): 225–42.

Fiebiger, Brett, and Marc Lavoie. 2018. “Unconventional Monetary Policies, with a Focus on Quantitative Easing*.” European Journal of Economics and Economic Policies: Intervention* 15 (2): 139–46.

FIS. 2021. “The Global Payments Report.”

Fong, Dick, Feng Han, Louis Liu, John Qu, and Arthur Shek. 2021. “Seven Technologies Shaping the Future of Fintech.”

Forstater, Maya. 2018. “Illicit Financial Flows, Trade Misinvoicing, and Multinational Tax Avoidance: The Same or Different.” CGD Policy Paper. Washington, DC: Center for Global Development.

Fraschini, Martina, Luciano Somoza, and Tammaro Terracciano. 2021. “Central Bank Digital Currency and Quantitative Easing.”

Frasher, Michelle. 2016. “Multinational banking and conflicts among US-EU AML/CTF compliance & privacy law: operational & political views in context.” Swift Institute Working Paper No. 2014-008.

Freixas, Xavier, Curzio Giannini, Glenn Hoggarth, and Farouk Soussa. 1999. “Lender of Last Resort: A Review of the Literature.”

Friedman, Benjamin M. 2008. “Why a Dual Mandate Is Right for Monetary Policy.” *International Finance*.

Friedman, Milton, and Allan Meltzer. 2022. “Money.” In *Encyclopedia Britannica*.

Friedman, Milton. 1969. *The Optimum Quantity of Money and Other Essays*.

Fritsche, Ulrich, and Ingrid Größl. 2007. “The Store-of-Value-Function of Money as a Component of Household Risk Management.”

Fulton, Colm. 2020. “Sweden starts testing world’s first Central Bank digital currency.” *The Reuters Journal.*

Fung, Ben S.C., and Walter Engert. 2017. “Central Bank Digital Currency: Motivations and Implications.” 2017–16. Ottawa. https://doi.org/10.34989/sdp-2017-16.

Gagnon, Joseph E. 2016. “Quantitative Easing: An Underappreciated Success.”

Gardin, Paul. 2019. “Should Central Banks Issue Digital Currencies? Consequences for the Financial System, Implications for Monetary Policy and Concerns for Privacy.” School of Public Affairs.

Garratt J., Maarten Van Oordt. 2021. “Privacy as a Public Good: A Case for Electronic Cash.” Journal of Political Economy 129 (7)

Georgiadis, Evangelos. 2019. “How Many Transactions per Second Can Bitcoin Really Handle? Theoretically.” Cryptology EPrint Archive.

Gnan, Ernest and Donato Masciandro. 2018. “Do We Need Central Bank Digital Currency?”Surf – The European Money and Finance Forum

Gnatenko, Iryna. 2020. “Potential Implications of the Introduction of CBDC for the Conduct of Monetary Policy and the Preservation of Financial and Monetary Stability.”

Goh, Brenda and Samuel Shen. 2019. “China’s proposed digital currency more about policing than progress”.*The Reuters Journal.*

Gong, X., Christy, M., Kem, Z., Chongyang, C., Matthew K. 2020. *"Cross- Side Network Effects, Brand Equity, and Consumer Loyalty: Evidence from Mobile Payment Markets."* International Journal of Electronic Commerce, 24:3, 279-304

Grathoff, Christian, and Thomas Moser. 2021. "How to Issue a Privacy-Preserving Central Bank Digital Currency."

Greenham, Tony, Andrew Jackson, Josh Ryan-Collins, and Richard Werner. 2011. *Where Does Money Come from: A Guide to the UK Monetary and Banking System*. New Economics Foundation.

Gross, Jonas, and Jonathan Schiller. 2021. "A Model for Central Bank Digital Currencies: Implications for Bank Funding and Monetary Policy *."

Gross, Jonas, Manuel Klein, and Philipp Sandner. 2020. "The Digital Euro and the Role of DLT for Central Bank Digital Currencies." Frankfurt.

Grothoff, Christian and Moser Thomas 2021. "How to issue a privacy-preserving Central Bank digital currency." SUERF Policy Briefs No 114

Group of Central Banks. 2020. "Central Bank Digital Currencies: Foundational Principles and Core Features (Report No 1)." Basel.

Group of Central Banks. 2021. "Central Bank Digital Currencies: System Design and Interoperability (Report No 2)." Report no 2. Basel.

Guo, Sky, Joseph Kreitem, and Thomas Moser. 2022. "DLT Options for CBDC."

Guofeng, Sun, and He Xiaobei. 2018. "Zero Lower Bound on Deposit Rates and Transmission Mechanism of the Negative Interest Rate Policy."

Hellman, Martin E. 1978. "An Overview of Public Key Cryptography."

Hoffman Samantha, John Garnaut, Kayla Izenman, Matthew Johnson, Alexandra Pascoe, Fergus Ryan, and Elise Thomas. 2020. "The Flipside of China's Central Bank Digital Currency Policy." International Cyber Policy Centre, ASPI.

Houben, Aerdt, and Klaus Löber. 2018. Committee on Payments and Market Infrastructures - Central Bank Digital Currencies.

Huang, Ying, Mayer Maximilian. 2022. "Digital currencies, monetary sovereignty, and U.S.–China power competition." Policy & Internet, 14, 324– 347.

Huang, Zhigang, Zhang, Tao. 2022. Blockchain and Central Bank digital currency. *ICT Express*, *8*(2), 264–270.

Huld, Arendse. 2022. "China Launches a Digital Yuan App- All You Need to Know." China Briefing, September 22, 2022.

IFRS. 2022. "Climate-Related Disclosures B Industry-Based Disclosure Requirements."

IMF. 2020. *A Survey of Research on Retail Central Bank Digital Currency*, (No. 20; 104).

IMF. 2022. “The Money Revolution: Crypto, CBDCs, and the Future of Finance.” Washington.

Ioannidis, Michael, Sarah Murphy, and Chiara Zilioli. 2021. “Occasional Paper Series The Mandate of the ECB: Legal Considerations in the ECB’s Monetary Policy Strategy Review.”

Iwańczuk-Kaliska, Anna. 2017. “Challenges for Central Banks in a Changing Payments Landscape.” *E-Finanse* 13 (2): 75–86.

Jones, Mark. 2022. “No One-Size-Fits-All Model for Central Bank Digital Currencies, IMF Head Says.” Reuters, February 9, 2022.

Khan, Ashraf, and Majid Malaika. 2021. “Central Bank Risk Management, Fintech, and Cybersecurity.” 21. 105. Washington.

Kahn, Charles M, Francisco Rivadeneyra, and Tsz-Nga Wong. 2018. “Should the Central Bank Issue E-Money?”

Kahn, Charles M, James Mcandrews, and William Roberds. 2004. “Money Is Privacy.” FRB of Atlanta Working Paper No. 2004-18.

Kajdi, László. 2022. “Working Paper Series Consumer Payment Preferences in the Euro Area.”

Kantar Public. 2022. “Study on New Digital Payment Methods.”

Keister, Todd, and Cyril Monnet. 2022. “Central Bank Digital Currency: Stability and Information.” *Journal of Economic Dynamics and Control 142* (September).

Khan, Ashraf, and Majid Malaika. 2021. “Central Bank Risk Management, Fintech, and Cybersecurity.” 21. 105. Washington.

Kiff, John, Jihad Alwazir, Sonja Davidovic, Aquiles Farias, Ashraf Khan, Tanai Khiaonarong, Majid Malaika, et al. 2020. “A Survey of Research on Retail Central Bank Digital Currency, WP/20/104, June 2020.”

Kim C., Tao W., Shin, N. and Kim, K.S. 2010. “An Empirical Study of Customers Perceptions of Security and Trust in E-Payment Systems.” Electronic Commerce Research and Applications, 9, 84-95.

Kim, Young Sik, and Ohik Kwon. 2019. “Central Bank Digital Currency and Financial Stability.”

Kochergina, D and Yangirovab, A. 2019. “*Central Bank Digital Currencies: Key Characteristics and Directions of Influence on Monetary and Credit and Payment Systems”*. Finance: Theory and Practice 23(4).

Kogan, Alexander, and Yunsen Wang. 2018. “Designing Confidentiality-Preserving Blockchain-Based Transaction Processing Systems.” International Journal of Accounting Information Systems 30: 1–18.

Kosse, Anneke, and Ilaria Mattei. 2021. *Gaining Momentum - Results of the 2021 BIS Survey on Central Bank Digital Currencies.*

Krasnova, Hanna and Veltri Natasha. 2010. "Privacy Calculus on Social Networking Sites: Explorative Evidence from Germany and USA". 43rd Hawaii International Conference on System Sciences, 2010, pp. 1-10.

Kshetri, Nir and Elena Loukoianova, 2022. “Data Privacy Considerations for Central Bank Digital Currencies in Asia- Pacific Countries.” Computer, vol. 55, no. 3, pp. 95-100.

Kubben, Pieter, Michel Dumontier, and Andre Dekker. 2019. “Fundamentals of clinical data science.” 219.

Kumar, Ananya. 2022. “A Report Card on China’s Central Bank Digital Currency: The e-CNY.” *Atlantic Council.*

Kumhof, Michael, and Clare Noone. 2018. “Central Bank Digital Currencies - Design Principles and Balance Sheet Implications.” Bank of England, Staff Working Paper No. 725.

Laboure, Marion, Markus H.-P. Müller, Gerit Heinz, Sagar Singh, and Stefan Köhling. 2021. “Cryptocurrencies and CBDC: The Route Ahead.” *Global Policy* 12 (5): 663–76.

Lagarde, Christine, and Fabio Panetta. 2020. “Report on a Digital Euro.” Frankfurt.

Laidler, David. 1969. “The Definition of Money: Theoretical and Empirical Problems.” *Source: Journal of Money, Credit and Banking*. Vol. 1.

Lee, Alexander. 2021. “What Is Programmable Money?” Board of Governors of the Federal Reserve System. Washington.

Lee, David Kuo Chuen, Yu Wang, and Li Yan. 2021. “A Global Perspective on Central Bank Digital Currency.” China Economic Journal 14 (1): 52–66.

Lima, Larissa de, and Erica M Salinas. 2022. “Retail Central Bank Digital Currency: From Vision to Design.”

Linck, K., Pousttchi, K., & Wiedemann, D. G. 2007. “Security Issues in Mobile Payment from the Customer Viewpoint.” MPRA Paper No. 2923.

Liu, Xin, Qi Wang, Guangdong Wu, and Chenghu Zhang. 2022. “Determinants of Individuals’ Intentions to Use Central Bank Digital Currency: Evidence from China.” *Technology Analysis and Strategic Management*.

Liu, Zhuang, Michael Sockin, and Wei Xiong. 2020. “Data Privacy and Temptation.”. NBER Working Paper 27635.

Long, Rui, Qingqing Wu, Neal N. Xiong, Meiqi Zhou, and Wei Zhou. 2019. “Delegated Proof of Stake with Downgrade: A Secure and Efficient Blockchain Consensus Algorithm with Downgrade Mechanism.” IEEE Access 7: 118541–55.

Lorran Da Silva, Augusto. n.d. “CDBC DESIGN FEATURES AND ITS POSSIBLE USE AS AN INSTRUMENT OF MONETARY POLICY.”

Luburić, Radoica, and Milena Vučinić. 2022. “Fintech, Risk-Based Thinking and Cyber Risk.” Journal of Central Banking Theory and Practice 11 (2): 27–53.

Lyons, Richard K, and Viswanath Ganesh Natraj. 2020. “What Keeps Stablecoins Stable?” 27136. Cambridge.

Ma, Chao Qun, Yi Shuai Ren, and Yi Ran Wang. 2022. “A Model for CBDC Audits Based on Blockchain Technology: Learning from the DCEP.” Research in International Business and Finance 63 (December).

Macgillivray, Alexander, Nik Marda, and Alondra Nelson. 2022. “Technical Design Choices for a U.S. Central Bank Digital Currency System.” Tennessee.

Malhotra, Diksha, Poonam Saini, and Awadhesh Kumar. 2022. “How Blockchain Can Automate KYC: Systematic Review.” Wireless Personal Communications 122: 1978-2021.

Mancini-Griffoli, Tommaso, Maria Peria, Itai Agur, Anil Ari, John Kiff, Adina Popescu and Celine Rochon. 2018. “Casting Light on Central Bank Digital Currency.” IMF Staff Discussion Note, 18/08.

Manolache, Manuel Adelin, Sergiu Manolache, and Nicolae Tapus. 2021. “Decision Making Using the Blockchain Proof of Authority Consensus.” In Procedia Computer Science, 199:580–88. Elsevier B.V.

Mclaughlin, Jeremy M, Philip J Morgan, and Kai Zhang. 2022. “MiCA-Overview of the New EU Crypto-Asset-Regulatory Framework.”

Mell, Peter, Nik Roby, Karen Scarfone, and Dylan Yaga. 2018. “Blockchain Technology Overview.” Journal of Research of the National Institute of Standards and Technology, June, 1–75. https://doi.org/10.6028/NIST.IR.8202.

Milunovich, George. 2022. “Assessing the Connectedness between Proof of Work and Proof of Stake/Other Digital Coins.” Economics Letters 211 (January): 1–4.

Moenjak, Thammarak. 2014. *Central Banking: Theory and Practice in Sustaining Monetary and Financial Stability.*

Mogensen, Samuel Eddie, Søren Truels Nielsen, and Julia Weismann Seixas. 2022. “New Types of Digital Money.” Copenhangen.

Mondal, Prakash, Rupam Deb and Mohammad Nurul Huda. 2016. “Know your customer (KYC) based authentication method for financial services through the internet.” 19th International Conference on Computer and Information Technology (ICCIT), 535-540.

Mu, Angela and Yibin Mu. 2022. “CBDC: Concepts, Benefits, Risks, Design, and Implications.”

Mu, Changchun. 2022. “Balancing Privacy and Security: Theory and Practice of the E-CNY’s Managed Anonymity.” Beijing.

Murakami, David, Ganesh Viswanath Natraj, and Ivan Shchapov. 2022. “CBDCs, Financial Inclusion, and Optimal Monetary Policy.” SSRN Electronic Journal, October 1–69.

Nakamoto, Satoshi. 2008. “Bitcoin: A Peer-to-Peer Electronic Cash System.”

National Bank of Ukraine. 2019. *Analytical Report on the E-hrynvia Pilot Project*.

National Information Center. n.d. “Commercial Bank.” All Institution Types Defined.

Nations Department of Economic, United, Social Affairs Economic Analysis, and Policy Division. 2022. “World Economic Situation and Prospects: August 2022 Monthly Briefing.”

Nelson, Bill. 2018. “Financial Stability and Monetary Policy Issues Associated with Digital Currencies.” *Journal of Economics and Business 100* (November): 76–78.

Nick, Szabo. 1994. “Smart Contracts.” 1994.

Norbert, Michel. 2022. “Central Bank Digital Currencies Are About Control – They Should Be Stopped.” Forbes . April 12, 2022.

Olsen, O. 2018. “Central Bank digital currencies”, Norges Bank Papers, no 1, pp 5-31.

Ordonez, Miguel A. Fernandez. 2022. “Stablecoins Reserves Must Be 100% Central Bank Money.”

Organization for Economic Cooperation and Development (OECD). 2021. “Government at a Glace 2021 Country Fact Sheet.” OECD Economic Surveys.

Panetta, Fabio. 2018. “21st Century Cash - Central Banking, Technological Innovation and Digital Currencies.” SUERF Conference Proceedings 2 (June): 23–32.

Panetta, Fabio. 2022. “Policy Panel on Central Bank Digital Currencies.”

Panetta, Fabio. 2022. “The Digital Euro and the Evolution of the Financial System.” Brussels.

Paul, Pascal. 2022. “Banks, Maturity Transformation, and Monetary Policy.” *Journal of Financial Intermediation*, November, 101011.

PBOC. 2018. *Technical Aspects of CBDC in a Two-Tiered System*.

People’s Bank of China. 2021. “Progress of Research & Development of E-CYN in China”.

Piazzesi, Monika, and Martin Schneider. 2022. “Credit Lines, Bank Deposits or CBDC? Competition & Efficiency in Modern Payment Systems.”

Pocher, Nadia, and Andreas Veneris. 2021. “Privacy and Transparency in CBDCs: A Regulation-by-Design AML/CFT Scheme.” IEEE , June, 1–9.

Reis, Ricardo, and Silvana Tenreyro. 2022. “Helicopter Money: What Is It and What Does It Do? *.”

Rennie Ellie, and Stacey Steele. 2021. “Privacy and Emergency Payments in a Pandemic: How to Think about Privacy and a Central Bank Digital Currency.” Law, Technology and Humans 3 (1): 6–17.

Reuter, Peter. 2017. “Illicit Financial Flows and Governance: The Importance of Disaggregation.” World Development Report.

Riksbank Sveriges. 2021. “E-Krona Pilot Phase 1.”

Riksbank, Sveriges. 2022. “E-Krona Report E-Krona Pilot Phase 2.”

Riksbank. n.d. “Sveriges Riksbanken Is Founded.”

Risberg, Pearl, and Stephanie Segal. 2020. “Central Bank Digital Currency, Design Choices, and Impacts on Currency Internationalization.” Center for Strategic and International Studies, December 1–6.

Roberts, Andy. 2002. *“A Principles Complementarity of Method: In Defence of Methodological Eclecticism and the Qualitative- Quantitative Debate.”* HCAS Journal, Vol. 7 No. 3.

Rogoff, Kenneth, and Woodford Michael. 2015. “Cost and Benefits to Phasing out Paper Currency”. University of Chicago Press.

Saleh, Shuyu Lan, and Vaghoor Kashani. 2021. “Influence of E-Krona & e-CNY on Individual Privacy A Comparative Study between Sweden and China.”

Sands, Peter, Weisman, Benjamin, Campbell, Haylea, Keatinge, Tom. 2017. “Limiting the Use of Cash for Big Purchases: Assessing the Case for Uniform Cash Thresholds.” International Cash Conference No 25-27.

Schickler, Jack. 2022. “Sweden Wants to Test E-Krona Viability for Smart Payments.”

Shah, Dinesh, Rakesh Arora, Han Du, Sriram Darbha, John Miedema and Cyrus Minwalla. 2020. “Technology Approach for a CBDC.” Analytical Note 2020-6, Bank of Canada.

Shirai, Sayuri. 2019. “ADBI Working Paper Series MONEY AND CENTRAL BANK DIGITAL CURRENCY Asian Development Bank Institute.”

Shostack, Adam and Syverson, Paul. 2004. “What Price Privacy?”. Economics of Information Security. Advances in Information Security, Vol. 12.

Sisnett, Paul, Daniel Holden, and Amit Sharma. 2022. “A New Era for Money.”

Smaghi, Lorenzo Bini. 2009. “Conventional and Unconventional Monetary Policy.” *International Center for Monetary and Banking Studies*.

Strehle, Elias. 2020. “Public Versus Private Blockchains.” Working Paper Series No. 14. Hamburg.

Stuckey, H. 2013. “Three types of interviews: Qualitative research methods in social health”. Journal of Social Health and Diabetes, 1(29) 56-59.

Svergies Riksbank. 2018. *The Riksbank´s e-Krona project (Report 2)*.

The Royal Mint. n.d. “Legal Tender Guidelines.”

Tobin, J. 1987. “The case for preserving regulatory distinctions”, Proceedings of the Economic Policy Symposium, Jackson Hole, Federal Reserve Bank of Kansas City, pp. 167–83.

Turrin, Richard. 2022. “Digital Yuan (e-CNY) App Topping the Charts.” Turrin, Richard. 2022.

Union, European. 1957a. “Treaty on the Functioning for the European Union.” *Article 128.*

Union, European. 1957b. “Treaty on the Functioning for the European Union.” *Article 127.*

United Nations General Assembly. 1948. “Universal Declaration of Human Rights - Article 3.”

United States House of Representatives. 1926. “US Code.” *Title 31, § 5103. Legal Tender.*

Visa. 2022. “VisaNet: Catalyst for Commerce.” VisaNet. 2022.

Vitalik, Buterin. 2015. “On Public and Private Blockchains.”

Wahid, Pessarlay. 2022. “China: Bank Testing e-CNY Smart Contract-Enabled School Fee Payment in Sichuan.”

Wall Street Journal (WSJ). 2021. “Why China’s New Digital Currency Raises Privacy Concerns.”

WEF. 2022. “Privacy Concerns Loom Large as Governments Respond to Crypto.” World Economic Forum. April 14, 2022.

Whitesell, William. 2006. “Interest Rate Corridors and Reserves.” *Journal of Monetary Economics* 53 (6): 1177–95.

Williamson, Stephen D. 2022. “Central Bank Digital Currency and Flight to Safety.” *Journal of Economic Dynamics and Control* 142 (September).

Williamson, Stephen. 2022. “Central Bank Digital Currency: Welfare and Policy Implications.” Journal of Political Economy 130 (11).

World Bank. 2017. *Distributed Ledger Technology (DLT) and Blockchain Acknowledgments III.*

World Bank. 2021. “THE GLOBAL FINDEX DATABASE 2021: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19.

Xu, Jianguo. 2022. “Developments and Implications of Central Bank Digital Currency: The Case of China e-CNY.” Asian Economic Policy Review.

Yao, Qian. 2018. “A Systematic Framework to Understand Central Bank Digital Currency.” Science China Information Sciences 61 (3).

Appendix
Interview-guides and Reports

Interview Guide Sub- QR 3

Dear Participant,

We are pleased that you have agreed to participate in this interview guide, and we thank you very much for this. Without your contribution, this research would not be possible. You are making a great contribution to our master's thesis at the *NOVA School of Business and Economics.*

The purpose and objective of the study are to analyze the implications and challenges of a Central Bank Digital Coin (CBDC). One topic of our master's thesis focuses on privacy and illicit financial activities (e.g., money laundering, terrorist financing).

The interview is divided into two parts:

1) First, we would like to start with some general questions about yourself and your profession.
2) Subsequently, we would like to discuss with you the implications and challenges of Central Bank coins with regards to the three subjects mentioned above.

It goes without saying that we adhere to a high standard of data protection, so that the evaluation is anonymous and has no reference to society.

Declaration of consent

"I agree that the interview conducted with me may be used for the evaluation within the scope of the master's thesis. I have been assured that all personal data that could be used to draw conclusions about my person will be anonymized and that these data, as well as the interview guide, will be deleted after completion of the master's thesis."

• Do you agree?	○ **Yes**	○ **No**

Our interest is in gaining insight into your experiences and views on the topics covered in this interview. Thus, there are ***no right or wrong*** answers.

Part 1: General section

General questions about yourself and the expertise of the industry

Q1) Who is your current employer?	
Q2) What is your current position in the company?	

Q3) How many years have you been in the CBDC industry?	

Part 2: Discussion

We would like to proceed with the second part of the questions. We are interested in questions about the impact and challenges related to privacy and illegal financial activities, that ultimately helps answering our research question:

Implications and Challenges of CBDCs' Privacy: How to Safeguard Consumer Privacy without Facilitating Illicit Financial Activity?

Privacy and CBDC

First, we would like to hear your thoughts on the privacy aspect of a CBDC. We are interested in your perceptions of the challenges and drawbacks of dealing with privacy, as well as the benefits you believe a CBDC provides in terms of privacy. The principles of privacy and personal data protection are codified in law *in articles 7 and 8 of the Charter of Fundamental Rights of the European Union. "1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and based on the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right to know what information has been collected about them and to have it corrected. 3. Compliance with these rules shall be subject to control by an independent authority."*

Q1) What challenges or drawbacks do you think CBDCs might have with respect to privacy? (e.g., loss of identity, exposure of sensitive information, etc.)	Please type your answer here:

Please rate the following assertions about the lack of privacy in a CBDC on a scale of one to five, with 1 representing "strongly disagree" and 5 representing "strongly agree."

Q2) When a Central Bank coin is designed to lack privacy, does spamming, stalking, robbery, and identity theft occur?

Do not agree (=1)	○	○	○	○	○	Agree (=5)
	1	2	3	4	5	

Explanation? Explicitly ask for extreme results (1 and 5).

Q3) Compared to cash, what benefits does a CBDC have in terms of privacy? Does it provide the same privacy?	Please type your answer:
Q4) Do you believe it is feasible to design a CBDC in such a way that it is untraceable? If yes/no – main reasons?	Please type your answer:

Q5) Do you believe that a CBDC could be more trustworthy with or without legislative entrenchment? (e.g., enshrined in law as legal tender)	Please type your answer here and justify it:
Q6) What safeguards exist for privacy in a CBDC? (e.g., fundamental rights, data protection)	Please type your answer here:

Privacy and Illicit Financial Activity

Next, we would like to hear your take on several prospective approaches to protect privacy but also uncover illicit financial activity (e.g., money laundering, terrorist financing, etc.).

Q7) What capabilities do you see to ensure as much privacy as possible in a CBDC but still detect illicit financial activity (e.g., money laundering, terrorist financing)?	Please type your answer here:

Please rate the following assertions about potential solutions with respect to privacy and illicit financial activity on a scale of one to five, with 1 representing "strongly disagree" and 5 representing "strongly agree." Are the proposed solutions both feasible and reasonable?

Q8) **Technical design** could solve the problem (e.g., cryptographic techniques, token based CBDC, etc.).

Do not agree (=1)	○	○	○	○	○	Agree (=5)
	1	2	3	4	5	

Explanation? Explicitly ask for extreme results (1 and 5).

Q9) **Legislation** could solve the problem (e.g., changing the law, etc.)

Do not agree (=1)	○	○	○	○	○	Agree (=5)
	1	2	3	4	5	

Explanation? Explicitly ask for extreme results (1 and 5).

Q10) **Threshold or anonymity vouchers** could help solve the problem (e.g., transfer anonymity up to certain amount, use a voucher for anonymous transfer, etc.)

Do not agree (=1)	○	○	○	○	○	Agree (=5)
	1	2	3	4	5	

Explanation? Explicitly ask for extreme results (1 and 5).

Q11) Other **options** to safeguard privacy but detect illicit financial activity?	Please type your answer here:

That brings us to the end of the interview. We would like to ask you if there are any additional notes you would like to add to the topic we have discussed so far that have not yet been covered and that you would like to include.

Q12) What remarks on the topics discussed so far are there that have not yet been addressed and that you would like to add?	Please type your answer here:

We would like to thank you very much for your participation in our interview.

Interview Report for sub- RQ 3: Expert 1

Interviewee Information

Name
Anonymous

Position
Senior Payment Expert/ Innovation Hub

Date of Interview
26/10/2022

Purpose
This interview aims to understand the implications and challenges of CBDC's privacy and illicit financial activity. The objective of the interview is to evaluate the findings presented in the literature. The focus of the interview is to gain further insight into the above-mentioned topics and identify certain commonalities while naming distinctions to the scholarly view.

Main Insights and Recommendations

Theme 1: Privacy aspect of a CBDC

- Compared to cash, CBDC will always lose in terms of privacy
- Safeguards for privacy are existing data protection regulations, followed by technical design (pseudonymity and cyber resilience)
- Lack of privacy means lack protection for those involved in illicit activities
- CBDC need to bring a value add and privacy could be a deciding factor. There is a discrepancy between stated and revealed preference regarding privacy: Privacy is of the utmost importance for people, even though most people use Big Tech solutions.
- Legal Tender could help great acceptance of CBDC and also support the government in digitization.

Theme 2: Privacy and Illicit Financial Activity

- CBDC needs to fulfill AML/CTF regulations, as a CBDC should not be a haven for illicit activities
- Both extremes could lead to reputational damage, which Central Banks have to avoid at all costs. There is a fine line between privacy and AML/CTF, and there is a need to implement some kind of pseudonymity with the possibility for investigative authorities to get hold of the data after a digital search warrant issued by an independent judiciary (separation of powers is important)
- Make use of existing intermediaries and use their known capabilities to combat financial crime
- Technical innovations could help solve the issue (e.g., self-sovereign identities), but there are also techniques to avoid such as smurfing
- The main weight falls on the investigative authorities

Source: own illustration

Interview Report for sub- RQ 3: Expert 2

Interviewee Information

Name
Anonymous

Position

Senior Consultant Emerging Technologies / PhD on Central Bank Digital Currencies and cryptography

Date of Interview
28/10/2022

Purpose
This interview aims to understand the implications and challenges of CBDC's privacy and illicit financial activity. The objective of the interview is to evaluate the findings presented in the literature. The focus of the interview is to gain further insight into the above-mentioned topics and identify certain commonalities while naming distinctions to the scholarly view.

Main Insights and Recommendations

Theme 1: Privacy aspect of a CBDC

- CBDC should have a cash-like design, which depends on the technical design of a CBDC
- Traceability must be undermined, which would solve most of the privacy issues
- Technical concepts are available to protect privacy
- Cash will always have advantages in terms of privacy. However, technical design choices can be a means to make it more or less private.
- A CBDC should have legal tender status to gain wide acceptance in the first place. In addition, it should have simple regulated access, especially for older people (high acceptance).

Theme 2: Privacy and Illicit Financial Activity

- CBDC should have AML spending limits, technical capabilities could also be the integration of identity in the coin → should be built on a blockchain to avoid double-spending. In this case, the Central Bank would be the public ledger. It would be possible to verify what exists only once. In the process money laundering would also benefit.
- CBDC needs a good legal framework
- Threshold, for example, could not improve privacy, but the technical design
- ZKP, Blind signatures
- Illegal financial activity will always find its way – measures will not be enough to fully detect IFA

Source: own illustration

Interview Report for sub- RQ 3: Expert 3

Interviewee Information

Name
Anonymous

Position
Researcher and professor for CBDC, Business informatics

Date of Interview
01/11/2022

Purpose
This interview aims to understand the implications and challenges of CBDC's privacy and illicit financial activity. The objective of the interview is to evaluate the findings presented in the literature. The focus of the interview is to gain further insight into the above-mentioned topics and identify certain commonalities while naming distinctions to the scholarly view.

Main Insights and Recommendations

Theme 1: Privacy aspect of a CBDC

- Under the EU GDPR, financial data might be classified as sensitive information, that requires special care. Examples of such data could then be identity-related information (buyer and seller names, age, gender, address) and transaction-related information (purchased goods or services, price, purchase frequency).
- A lack of privacy would enable Central Banks, government to gather and process the data. The individual would therefore be in danger of stricter control and supervision by these actors and the government.
- Cash remains the most anonymous payment method, as no digital information is produced and stored.
- Privacy-enhancing technologies could be somewhat ensured by Blockchain/ DTL technology or even ZKP.
- CBDC needs a competitive advantage to be adopted by individuals. Privacy could be this advantage. Further problem: Most individuals are satisfied with their choice of payment.
- Most people are not aware of the concept of legal tender, and if people distrust CBDC they will likely distrust political, and legal governmental institutions such as Central Banks
- Most important safeguard: Privacy is declared as a fundamental right that does not guarantee that rights are violated or that they are enforced.
- CBDC should be designed in the beginning so that all actors are not able to gather information and make inferences from CBDC transactions.

Theme 2: Privacy and Illicit Financial Activity

- Research is lacking in this regard to detect IFA but protect privacy
- Options: only a certain number of transactions per entity could be transferred anonymously, while others would be transparent; the upper limit per transaction would be one option.
- Some solutions (e.g., token-based approach) come with other disadvantages, such as a decrease in payment speed or number of transactions per second.
- Central Banks will decide against Threshold/ Anonymity Vouchers looks unconventional and messy. If this were to be the only option, Central Banks would rather go for a more transparent CBDC

Source: own illustration

Interview Report for sub- RQ 3: Expert 4

Interviewee Information

Name
Anonymous

Position
Digital Law Team; prior: Audit with digital focus

Date of Interview
02/11/2022

Purpose
This interview aims to understand the implications and challenges of CBDC's privacy and illicit financial activity. The objective of the interview is to evaluate the findings presented in the literature. The focus of the interview is to gain further insight into the above-mentioned topics and identify certain commonalities while naming distinctions to the scholarly view.

Main Insights and Recommendations

Theme 1: Privacy aspect of a CBDC

- CBDC cannot have the same level of privacy as cash
- There is a need for continuous supervision of the enforcement of this regulation. That means that a CBDC should be designed in a way that all actors are not able to get sensitive information and can make inferences from a CBDC transaction data to perform activities against their wishes.

Theme 2: Privacy and Illicit Financial Activity

- Regular audits of government access to private transactions could be performed by an independent body explicitly designed to protect user privacy, which in turn could also monitor for potential AML/ CTF abuse.
- Technological innovation can be a means to balance these competing priorities, but technology is simply inadequate to avoid the misuse of this data if the government insists on the data.
- The assumption is that CBDC must comply with all these existing AML, CFT, and KYC rules, but this is not necessarily true. The regulations are statutory, but Congress could modify these obligations.
- There should be a more informed discussion of how privacy in CBDC should be preserved at the legal level, rather than solely relying on technology that might not have been tested in real-life scenarios

Source: own illustration

Interview Report for sub- RQ 3: Expert 5

Interviewee Information

Name
Anonymous

Position Alternate Member of the Governing Board/ Several papers on CBDCs

Date of Interview
04/11/2022

Purpose
This interview aims to understand the implications and challenges of CBDC's privacy and illicit financial activity. The objective of the interview is to evaluate the findings presented in the literature. The focus of the interview is to gain further insight into the above-mentioned topics and identify certain commonalities while naming distinctions to the scholarly view.

Main Insights and Recommendations

Theme 1: Privacy aspect of a CBDC

- Extremely difficult to get the same level of privacy in CBDC as with physical cash. As soon as people make payments digitally there will always be traces, and people leave some data.
- It is important to design a CBDC in the beginning in a way to preserve privacy (e.g., when you have a system, you cannot add features later on). Privacy has to be thought through in the design.
- Still somewhat controversial, as data and privacy can still be abused.
- Privacy is declared to be a fundamental right and, in the legislation

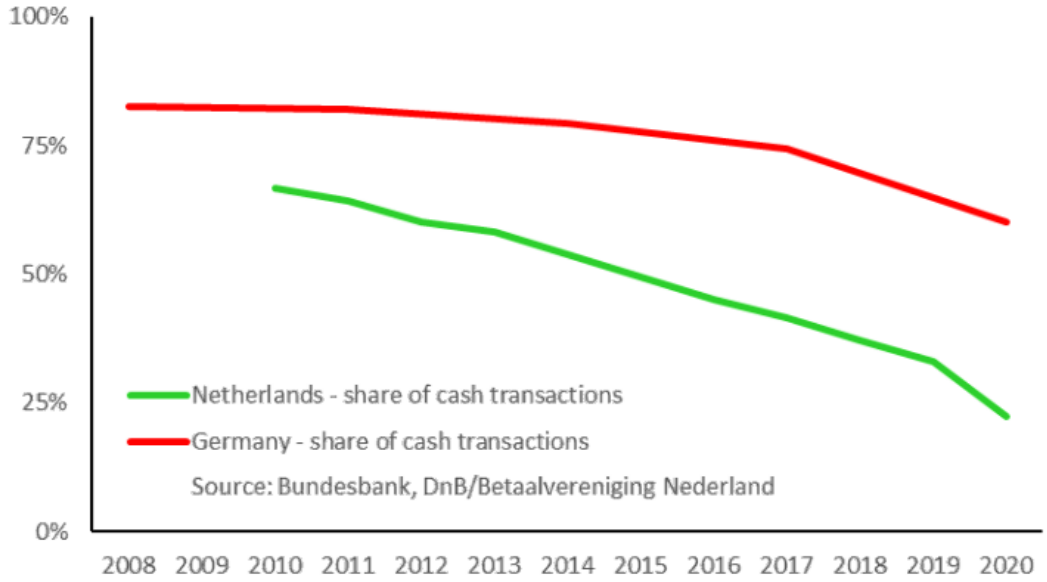
Theme 2: Privacy and Illicit Financial Activity

- One way to get privacy but detect illicit financial activity is through asymmetric privacy. Total anonymity when someone pays, but not as a receiver. Through that, there might be options to prevent illicit use, as the receiver is always visible and cannot avoid taxes. That would also protect the buyer, as no one should know what the buyer is purchasing. This option would be less private than cash, but a payer would have total anonymity.
- Other cryptographic techniques, such as a "whitelist". In that case, people have to preregister, meaning to be whitelisted, where ZKP could help identify that people are on that so-called "while list". Different idea from what is otherwise suggested or even required of regulators.
- Other options: Cryptographic techniques (e.g., distribute keys)
- Parliamentary committed to overview governments, but history tells that it usually doesn't work well.

Source: own illustration

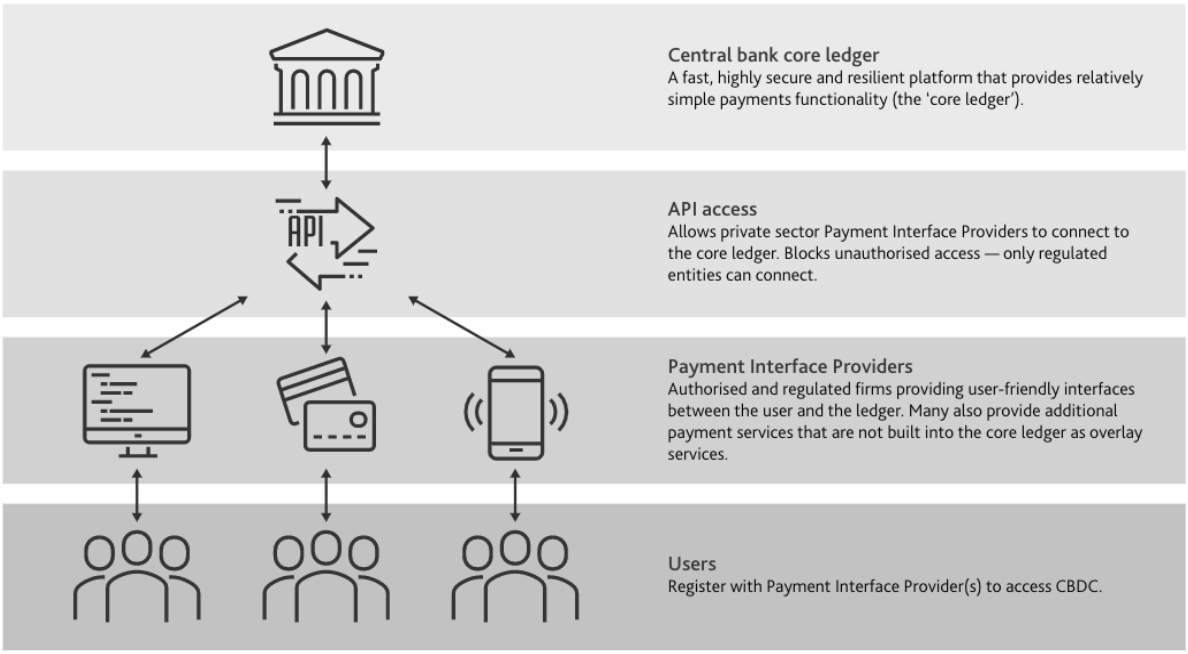
List of Figures

Figure I: Cash usage evolution in the Netherlands and Germany (% of total transactions).



Source: Bundesbank, DnB/Betaalvereniging Nederland in Panetta, Fabio. 2022. "Policy Panel on Central Bank Digital Currencies."

Figure II: Platform Model of a CBDC.



Source: Bank of England. (2020). "Central Bank Digital Currency Opportunities, challenges and design

List of Tables

Table I: Current Status of CBDC projects

Digital Currency	Country/Region	Central Bank(s)	Announcement year	Status	Retail/Wholesale	Structure	DLT/Non-DLT	Main goals of the CBDC
Sand Dollar	Bahamas	Central Bank of Bahamas	2022	Launched	Retail	Token	DLT	The CBB is to add more features to the next version of the Sand Dollar's 'core application' to allow financial institutions to "seamlessly structure and manage merchant fee arrangements"
e-CNY	China	People's Bank of China	2022	Pilot	Retail	Account	Non-DLT	The main goal of e-CNY to provide a convenient, yet more efficient and secure retail payment system to increase financial inclusion, preserve monetary sovereignty, and to provide a "back up" payment infrastructure for the private sector payment solutions. Further, fair competition and interoperability should be promoted.
Dinero Eletronico	Ecuador	Central Bank of Ecuador	2017	Cancelled	Retail	Account	Non-DLT	Electronic money will not only help the poor but will act as a cost-saving mechanism for the government: Ecuador spends more than $3 million every year to exchange deteriorating old notes for new dollars.
Digital Euro	Euro Area	European Central Bank	2022	Research	Retail/Wholesale	Account/Token		A digital euro could support the Euro system's objectives by providing citizens with access to a safe form of money in the fast-changing digital world.
e-Naira	Nigeria	Central Bank of Nigeria	2022	Pilot	Retail		DLT	The aim is to increase efficiency in cross-border payments, increase financial inclusion, facilitate remittances, and reduce informality
e-Krona	Sweden	Sveriges Riksbank	2017	Proof of Concept	Retail	Account/Token	DLT	The main goal of the e-krona is to counteract the declining use of cash and increase financial stability
USA CBDC	United States of America	US Federal Reserve	2022	Research	Retail/Wholesale		DLT	

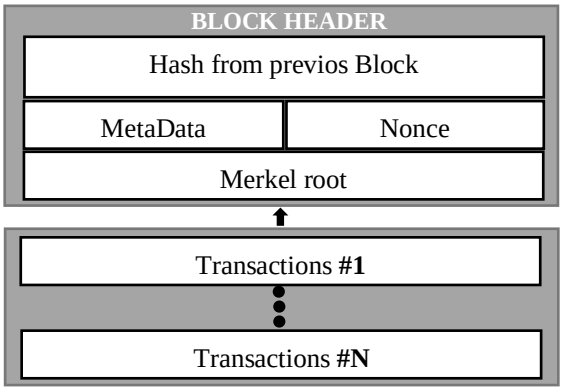
Source: CBDC Tracker. 2022. "Today's Central Bank Digital Currencies Status." CBDC Tracker. December 8, 2022. https://cbdctracker.org/.

Table II: Blockchain Fundamentals.

Blockchain Features (I)	Qualities of Blockchain (II)
Block (see. Bitcoin Block III) Block Header – Metadata (…) Transaction Data **Node (N.) = computer connected to network** Full N. – store date; ensures transaction validity Lightweight N. – no storage of data; pass to full n. **Ledger = Database** Records transaction history **Public-Key-Cryptography (PKC)** Encrypt and Decrypt Data	**Security** Cryptographically secured **Resiliency** Fault tolerance; copies of the entire BC **Immutability** Append-only; read and write **Transparency** Visible to all participants **Verifiability** U. able to verify each b. independently

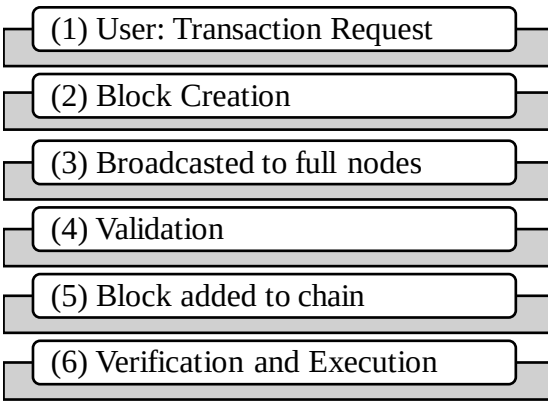
Source: Anwar, Hasib. "The Ultimate Blockchain Technology Guide: A Revolution to Change the World."

Structure of a Block, e.g., Bitcoin (III)

BITCOIN BLOCK	DESCRIPTION
	• **Hash from previous block** Connection to previous block • **Metadata** Block version number Time stamp & Difficulty • **Nonce** Number used once • **Merkle Root** Summary of all transactions • **Transactions per block** Full nodes save all transactions

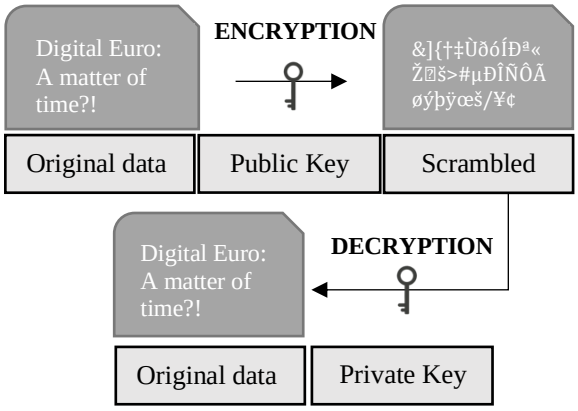
Source: Marc Steiner. "Description of Bitcoin Blocks and Transactions."

Transaction Process: Step-by-Step View (IV)



Source: Medium, "Smart Contracts the Key of Web3."

Public-Key Cryptography, PKC (V)



Source: IBM, "Public Key Cryptography."

Table III: Types of Blockchain Technology.

Feature	Public	Private	Consortium/ Federal
Consensus Determination	All miners	One organization	Selected set of nodes
Access	Permissionless	Permissioned	Permissioned
Efficiency	Low	High	High
Transaction Speed	Slow	Fast	Fast
Centralized	No	Yes	Partial

Notes: Overview of the main blockchain types.
Source: Adopted from Zheng et. al 2018b, "Blockchain Challenges and Opportunities: a survey".

Table VI: Overview of interviewees for sub- RQ 3.

No.	Interviewee	Position	Organization	YOE
1	E1	Senior Payment Expert/ Innovation Hub	Deutsche Bundesbank	8+
2	E2	Senior Consultant Emerging Technologies / PhD on Central Bank Digital Currencies and cryptography	Ernst & Young	6+
3	E3	Researcher and professor for CBDC, Business informatics	Goethe University Frankfurt	4+
4	E4	Digital Law Team; prior: Audit with digital focus	Ernst & Young	7+
5	E5	Alternate Member of the Governing Board	Swiss National Bank	10+

Glossary

Articles and Regulation	Definition and Explanation
Monetary System	
Article 128 of the Treaty on the Functioning for the European Union (TFEU 1957, 1)	"1. The European Central Bank shall have the exclusive right to authorize the issue of euro banknotes within the Union. The European Central Bank and the national Central Banks may issue such notes. The banknotes issued by the European Central Bank and the national Central Banks shall be the only such notes to have the status of legal tender within the Union."
Title 31 – Money and Finance § 510. Legal Tender (US Code, 1926)	"United States coins and currency (including Federal reserve notes and circulating notes of Federal reserve banks and national banks) are legal tender for all debts, public charges, taxes, and dues. Foreign gold or silver coins are not legal tender for debts."
Central Bank Functions	
Article 127 of the Treaty on the Functioning for the European Union (TFEU 1957, 1)	1. The primary objective of the European System of Central Banks (hereinafter referred to as 'the ESCB') shall be to maintain price stability. Without prejudice to the objective of price stability, the ESCB shall support the general economic policies in the Union with a view to contributing to the achievement of the objectives of the Union as laid down in Article 3 of the Treaty on European Union. The ESCB shall act in accordance with the principle of an open market economy with free competition, favoring an efficient allocation of resources, and in compliance with the principles set out in Article 119.

Privacy and Data Protection	
Article 7 and 8 in the Charter of Fundamental Rights (CFR 2007). Article 8 of the Convention for the protection of human rights and fundamental freedoms (ECtHR 1950).	"1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and based on the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority". Right to respect for private and family life "1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."
Article 12 of the Universal Declaration of Human Rights (UNGA 1948).	"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."
General Data Protection Regulation (GDPR) (EC and EUCO 2016)	"EGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)" *Note: Official version of the GDPR is 261 pages long.*

Technical Terms	
Blind signatures	Blind signatures allow a user to obtain a signature from a signer without learning anything about the message that the user signed or the contents of the message. The user can obtain a valid signature only after interacting with the signer once. *Source: Chaum David. 1982." Blind signatures for untraceable payment" Advances in Cryptology.*
Zero – knowledge proof	In simple terms, a zero-knowledge proof is a technique in which one entity, the so- called prover may prove something to another entity, the so- called verifier without giving any information other than the fact that that specific assertion is true. In that case, the proofer is just getting limited or no information. *Source: Feige, Uriel, Amos Fiat, Adi Shamir. 1988. "Zero- Knowledge Proofs of Identity". Journal of Cryptology 1:77-94.*
Self – sovereign identities	Self- sovereign identities are defined as "a specific approach within the digital identity concept that empowers the individual to hold their credentials and issue specific consent to share them." (IOHK 2021, 6) *Source: IOHK. 2021." What is decentralized identity?"*