STOCKHOLM SCHOOL OF ECONOMICS

M.SC. FINANCE THESIS

The Role of Digital Identity in Building Central Bank Digital Currencies and the Direction this Development is Going

---

IEVA BRUZAITE

41951

SUPERVISOR: PROF. PAOLO SODINI

02/12/2022

Abstract

Recent years have witnessed an influx of private digital currencies. The ease of creation of private cryptocurrencies has raised concerns about the stability of the entire financial system. The decline of cash usage, the entrance of big tech into the financial sector and the emergence of cryptocurrencies have prompted central banks to start working on the central bank digital currencies (CBDCs) that can be seen as a way for central banks to maintain control in the monetary system. As CBDCs are still in their early stage, the trajectory of their design still has many unknowns. In this paper, it was evaluated that retail CBDCs being accessible to the general public can have the most impact. Besides, CBDC has to be tied to digital identity to ensure regulatory compliance, prevent illicit finance and account for the traceability of digital transactions. Digital identity is central to the efficient design of CBDC, but it is also at its early stages of development. The progress in the digital identity space has been slow and there may not be a one-fits-all solution, but it is vital to establish unifying standards for both CBDC and digital identity to ensure interoperability and efficiency. A decentralised digital identity that gives control of their data to the users shows a lot of potential and can tackle some of the key concerns in the CBDC design, such as privacy. CBDC and digital identity both are new concepts but can have a major impact on the financial sector and beyond, and both need to develop simultaneously to ensure their efficiency and maximise the benefits they can bring.

Declaration

I, Ieva Bruzaite, declare that the work contained in this thesis has not been submitted for any other degree or professional qualification. It represents my own work and the work of others is properly acknowledged and referenced. The work was carried out under the supervision of Professor Paolo Sodini between September 2022 and December 2022.

Word count: 16,316

Acknowledgements

First, I would like to thank my supervisor Professor Paolo Sodini for giving me an opportunity to work with him and helping me in the progress to find the right direction and being open to exploring the new concepts of CBDCs and digital identity.

Second, I would like to thank Ms Gabriela Guibourg from Riksbank for finding time to share her insights during the interview dedicated to this thesis. Her answers helped to understand better where both CBDC and digital identity stand and, in this way, contributed to this thesis.

Finally, I would like to thank Hjalmar Didrikson for suggesting the topic of digital identity and motivating me to explore this concept. I would like to thank the whole Alfvén & Didrikson team for their constant support and curiosity in my thesis.

Table of Contents

List of Figures

List of Tables

Abbreviations

Term	*Definition*
AE	*Advance Economy*
AML	*Anti Money Laundering*
BIS	*Bank For International Settlements*
CBDC	*Central Bank Digital Currency*
CDD	*Customer Due Diligence*
CFT	*Counter Financing of Terrorism*
DLT	*Distributed Ledger Technology*
eIDAS	*electronic Identification, Authentication and trust Services*
EMDE	*Emerging and Developing Economy*
ESCB	*European System of Central Banks*
GDPR	*General Data Protection Regulation*
FPS	*Fast Payments Service*
KYC	*Know Your Customer*
PKI	*Public Key Infrastructure*
PSP	*Payment Service Provider*
ZKP	*Zero Knowledge Proof*

Introduction

Over the last decade, we observed a skyrocketing interest in Fintech that brought a wave of innovation into the financial sector, later to be followed by the boom of cryptocurrencies that are yet to establish what long-term position they will take in the financial system. The digital finance landscape is indeed changing rapidly with now central banks and governments entering the playing field to establish their own central bank digital currencies (CBDCs). This move can be seen as a way to counter the overwhelming issuance of private cryptocurrencies, as this occurrence has become somewhat of 'the wild west' of the payments system.

Yet establishing CBDC is a significant deed and challenging task given that it must prevent criminal activities, ensure privacy, comply with data protection regulations and offer a good user experience to reach mass adoption. While there may not be a one-fits-all solution, the standards that can harmonize the development of CBDCs are vital to ensure technical and economic interoperability. The majority of central banks have not made any definite decisions regarding the design of CBDCs and it is crucial to maintain adaptability to keep up with technology advancements and build widely adaptable solutions. It has been widely discussed among researchers and policymakers that CBDC needs to be tied to digital identity. As our weakening and ageing identification systems are under more pressure to keep up with compliance demands, while also preventing fraudulent activities in the digital space, this calls to reconsider how we can identify ourselves in digital and physical space in the future. Digital identity can be way more than just our government-issued documents in an electronic form. It can encompass several layers of our identity, from legal documentation to behavioural insights such as how we interact with various platforms. While both CBDC and digital identity can have a major impact on risk management and market integrity, to achieve their full potential, both have to develop and innovate simultaneously.

The purpose of this paper is to evaluate the current state of CBDC and digital identity around the world, analyse existing research to highlight key characteristics and technology that will define the future of CBDC and digital identity, and indicate the direction in which they will develop. It has become clear that many countries still have not established clear design choices, and policy has a major role to play in defining it.

The paper starts with a discussion of digital currencies in general and later follows with a deeper dive into CBDC. The second part of the discussion covers digital identity and

analyses some of the characteristics that are relevant to its future development of it. Finally, both CBDC and digital identity are discussed together and finished with recommendations for future research. The paper also includes insights from the interview with Gabriela Guibourg, Head of Analysis and Policy at the Payments department at Sveriges Riksbank, to bring expert opinion and the newest insights.

1. Digital currencies

Digital currency (or digital money) can be described as a type of currency that can only be available in digital or electronic form. While society has had access to digital money for decades in the forms of claim-based money such as debit cards or payment platforms, (e.g., AliPay, Paypal), over the recent years, especially with the pandemic accelerating digitization, other forms of digital currencies, namely CBDC, cryptocurrencies, and stablecoins have gained significant attention. And while the world of digital currencies is swiftly evolving, and might shake up the entire global economy, there seems to be a lot of confusion about different types of digital currencies, their underlying motivations and design choices.

The first type of cryptocurrency emerged in 2008 when an alleged group or an individual under the alias Satoshi Nakamoto introduced the concept of Bitcoin. Nakamoto's intention was for the traditional bank to become redundant, and Bitcoin was a possible solution, based on a decentralised architecture and allowing peers to send money to each other instantly and without any intermediaries (Nakamoto, 2008). While given its flaws and inefficiencies Bitcoin is unlikely to become the future of money, it pointed out the latent demand for change, bringing attention to the feasibility of an alternative to the state-issued, interest-bearing 'fiat' currency money system that has been in place for decades (Birch, 2014). As over the past decade, the issuance of private cryptocurrencies skyrocketed, the confusion around them has also grown significantly. This led central banks around the world to worry about the financial stability of the global monetary system with more private cryptocurrencies being minted while having no regulation to supervise and control them. The Federal Reserve Governor Lael Brainard (2021) stated: "A predominance of private monies may introduce consumer protection and financial stability risks because of their potential volatility and the risk of run-like behaviour. Indeed, the period in the nineteenth century when there was active competition among issuers of private paper banknotes in the United States is now notorious for inefficiency, fraud, and instability in the payments system. It led to the need for a uniform form of money backed by the national government." In fact, the history of money indicates that the broad tendency has been in the direction of one currency for each political jurisdiction and common economic space, where in practice those political and economic spheres coincide (Eichengreen, 2019). From fragmented polities where feudal lords minted their own money in the Middle Ages, to commercial banks being able to issue notes alongside

central banks in the 17-19th centuries, to finally the power of money issuance becoming concentrated solely in the hands of central banks in the 19-20th centuries. A uniform currency minimized transaction costs and substituted for information, as it was not necessary to have information about the creditworthiness of every issuer, since there was only one. Hence central or federal governments sought to control the issuance of currency (Eichengreen, 2019).

1.1. Different types of digital currencies

Adrian & Mancini-Griffoli (2019) provides an overview of different types of digital currencies (*Figure 1*) by putting digital money into five different segments, namely, CBDC, Cryptocurrency, B-money, E-money, and I-money. Claim-based digital money is more familiar to society, even though E-money (Paxos, USD-Coin, TrueUSD), as well as I-money (Diem, prev. Libra), are fairly new concepts. Nevertheless, a lot of current discussions revolve around CBDC and Cryptocurrency which both fall into the object-type segment.

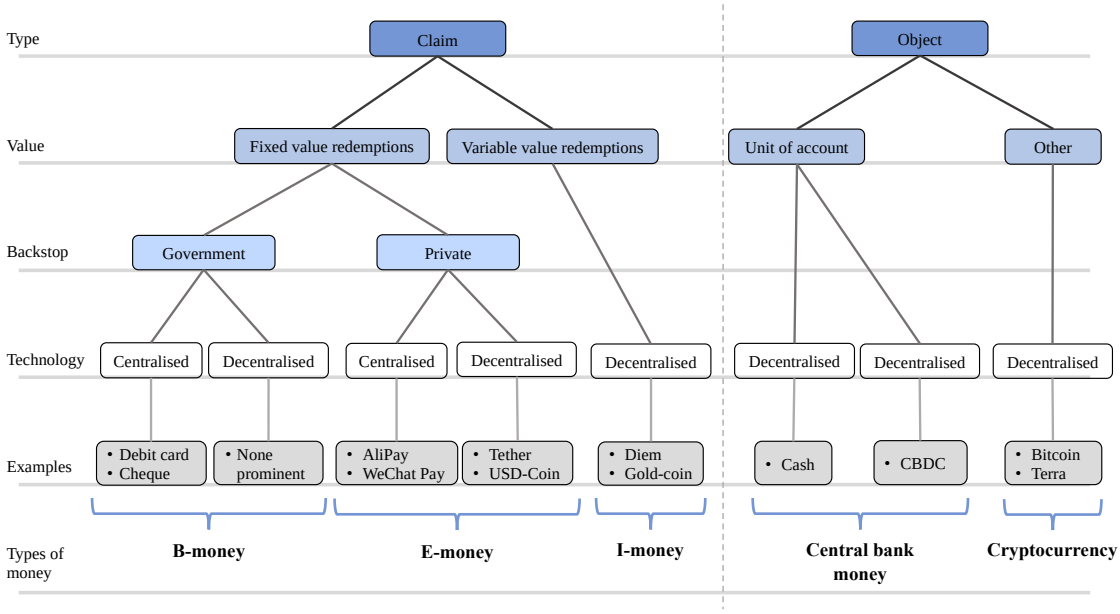

Figure 1: Types of digital money (Adrian & Mancini-Griffoli, 2019)

B-money typically covers commercial bank deposits and is associated with debt-like instruments denominated in a unit of account, redeemable upon demand at face value (Adrian & Mancini-Griffoli, 2019). Being by far the most widespread use of claim money, B-money (e.g. debit cards, wires, and checks) are usually carried through

centralised technology and backstopped by governments. **E-money** can be either private centralised payment solutions (e.g. AliPay, WeChat, M-Pesa) or tokens pegged to fiat currency (e.g. Tether, USD Coin, Gemini). Fiat tokens are cryptocurrencies with issued claims that can be redeemed in fiat currency at face value upon demand (Adrian & Mancini-Griffoli, 2019). Fiat tokens are often referred to as stablecoins, the term that is widely and vaguely used these days. Unlike B-money, E-money does not have redemption guarantees that are backstopped by governments. **I-money** is based on the same model as E-money, except for one critical feature – offering variable value redemptions into currency, thus, becoming an equity-like instrument (Adrian & Mancini-Griffoli, 2019). It can be backed by assets such as gold or stocks. One prominent example of I-money is Diem (prev. Libra) which entailed a claim on a portfolio of assets, namely, bank deposits and short-term government securities. I-money is also often classified as stablecoins. While I-money shows potential as a new means of payment, it is yet to show whether it can take off and given that Diem (prev. Libra) project was shut down, it signals many obstacles it still needs to overtake. Catalini & de Gortari (2021) point out that such investment tokens only have value as long as their ecosystem is thriving. Given that "the expectations were to change, such stablecoins would rapidly enter a death spiral and their coins would become worthless like banknotes issued by an unsound currency board" (Catalini & de Gortari, 2021). **Central Bank Digital Currency (CBDC)** is a digital form of currency backed by a central bank with legal tender status, meaning it can be used to settle debts or meet financial obligations (Duffie, et al., 2021). While countries like the Bahamas, Nigeria, Jamaica and the Caribbean nations have already launched their national CBDCs, there is an ongoing discussion on how CBDCs should be designed and there is a number of questions to be answered before CBDCs can reach a wider scale implementation. Soderberg (2022) points out that, as CBDC remains a fairly unchartered territory, increased international information-sharing of insights learned from individual CBDC projects and cooperation on the policy as well as design issues is vital for going forward. **Cryptocurrency** is, just like CBDC, another object-based means of payment. It is denominated in its own unit of account, created (or minted) by nonbanks, and issued on a blockchain, commonly of the permissionless type. Examples of such cryptocurrencies include Bitcoin and Ethereum. The cryptocurrency boom between 2017 and 2021 witnessed an influx of private cryptocurrencies. Although limited in supply, people held cryptocurrency either as a medium of exchange or as an investment asset class (Ozili, 2022). Managed coins that are usually also referred to as stablecoins are the

type of cryptocurrencies that rely on an algorithm to stabilize their value based on supply and demand by issuing more coins when their price is high and withdrawing coins from circulation when the price is lower, in this case aiming to maintain a stable price. Terra stablecoin which can be referred to as managed coin, experienced a total crash in its value (*Figure 2*), shedding $60 billion in market value, just in May 2022 (Sandor & Genç, 2022). This recent failure indicates that such 'stablecoins' are far from stable and are yet to show whether they can prove their validity and feasibility.

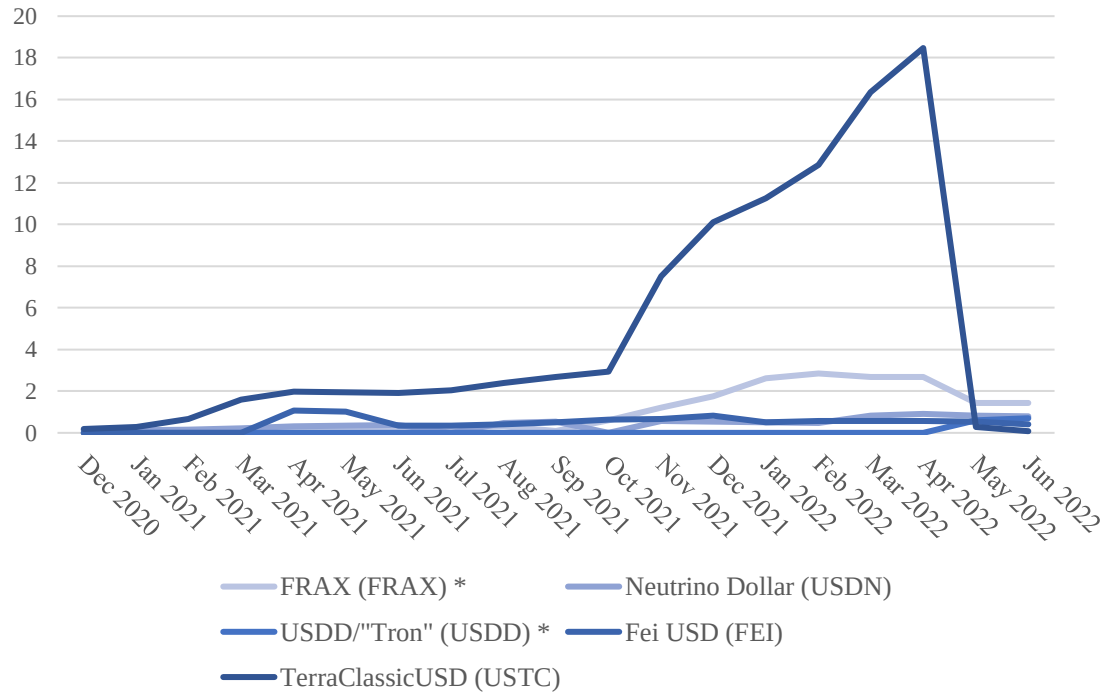

Figure 2: Market size of the algorithmic stablecoins (in billion USD) (Statista, 2022)

When it comes to the risk profile of discussed digital monies, CBDC can be considered the safest asset, since it is a unit of account provided by a central bank, thus, making it a stable store of value. Backstop by the government provides B-money with safety as a store of value. The stability of E-money comes from the guaranteed redemption at face value (Adrian & Mancini-Griffoli, 2019), but as E-money does not benefit from the government backstops, it relies on the strength of a balance sheet of an issuer. Given such conditions, E-money may be subject to run-risk. Equity-like instruments such as I-money directly inherit the risk of their underlying assets. I-money backed by government bonds will be less risky than I-money backed by stock market shares (Adrian & Mancini-Griffoli, 2019). BIS (2021) also indicates that cryptocurrencies are speculative assets

rather than money, and in many cases are used to facilitate money laundering, ransomware attacks and other financial crimes. Besides, cryptocurrencies based on the early blockchain architectures such as Bitcoin have few redeeming public interest attributes when also considering their wasteful energy footprint. For example, in early June 2021, the estimated annualised electricity consumption of the Bitcoin network (103.4 TWh per year) was roughly the same as that of the Netherlands (116.3 TWh per year) (The Cambridge Centre for Alternative Finance, 2021).

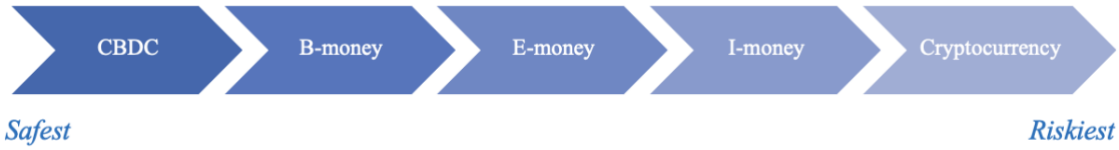

Figure 3: Risk profiles of digital money

1.2. Stablecoins

Stablecoins are designed to maintain stable value and may have a higher potential than other, unbacked crypto assets to be used for payments or to store value (Kosse & Mattei, 2022). Currently, the most popular use of stablecoins is to quickly switch between a volatile cryptocurrency and a theoretically more stable asset. For example, if a trader holds Bitcoin and expects its price to fall, they can almost instantly trade their Bitcoin for a stablecoin to protect their holdings. Stablecoins also enable cryptocurrency exchanges that do not support fiat currency trading to list an asset with a more stable value (Wind, 2019). In theory, stablecoins could provide the standard benefits of cryptocurrency without bringing price volatility into the picture. Nevertheless, the credibility of stablecoins is only as good as the governance behind the promise of the backing (BIS, 2021). What is clear from drawing the borders between different types of digital currencies, is that the term 'stablecoin' is being used very liberally and vaguely, and thus, falling into three different segments of digital currencies, namely E-money, B-money, and cryptocurrencies. Indeed, Catalini & de Gortari (2021) highlight that the word stablecoin has become "somewhat of a misnomer", as it is currently being used for a range of coins with significantly varying economic and technical properties. It ranges from coins that are fully backed by traditional currencies to algorithmic stablecoins that often lack transparency and are unlikely to withstand extreme market conditions (Catalini & de Gortari, 2021).

To make the distinction clearer, *Table 1* shows an overview of three different types of so-called stablecoins that have been taken into analysis, with one of each falling into a different segment of digital currencies, as presented by (Adrian & Mancini-Griffoli, 2019).

	Tether	Diem (prev. Libra)	Terra (UST)
State	Functional	Cancelled	Collapsed
Type	E-money	I-money	Cryptocurrency
Establishment year	2014	2019	2018
Reference asset	Fiat currency (1:1 US dollar)	A reserve of real assets (e.g., bank deposits and short-term government securities)	Uncollateralized and rely on algorithmic supply adjustments
Redemption rights	Fixed redemption	Variable redemption	Variable redemption
Stability	100% collateralization is meant to ensure price stability	Equity-like assets are susceptible to volatility	Vulnerable to bank runs and unlikely to sustain extreme conditions
Price fluctuations	1 year Low $0.9485/ High $1.00	Project suspended	1 year Low $0.00001675/ High $119.18 (price collapsed in May 2022)
Price	$0.999 *(22 November 2022)*	Project suspended	$0.0001601 *(22 November 2022)*
Market cap	$65,446,344,363 *(22 November 2022)*	Project suspended	$956,201,475 *(22 November 2022)*, before the collapse, reached $40 billion

Table 1: A comparison of different stablecoins (CoinMarketCap, 2022; Tether, 2014; Libra Association, 2019; Kereiakes, et al., 2019; d'Avernas, et al., 2022; Gross, 2019)

Stablecoins can be seen as a privately-issued counterpart to CBDC. As fiat stablecoins are backed one-to-one by central bank-issued assets, they may be considered by some central banks as an alternative (Soderberg, 2022) or even a competitor to CBDC (Catalini, et al., 2021). As stablecoins are gaining momentum, with the lack of regulation and insufficient risk management, they can constitute a threat to financial stability (Arner, et al., 2020; Kosse & Mattei, 2022). Stablecoins have the potential to fragment the liquidity of the monetary system and detract from the role of money as a coordination device (BIS, 2021). However, Catalini, et al. (2021) indicates that both stablecoins and CBDC can not only co-exist but also complement each other based on the relative strengths of the public and private sector. Balanced coexistence of stablecoins and CBDC can extend a public-private partnership in a way that fosters healthy competition, more choice for consumers and improved public services (Catalini & Massari, 2021). As CBDC projects remain in the early stages of their development, stablecoins are already in circulation with approximately $150 billion market value (Statista, 2022).

1.3. Central bank digital currencies

Given the apparent ease with which cryptocurrencies can be created, one must wonder whether they now reverse this trend towards uniformity, and central banks could see this as a potential danger. The ongoing digital revolution can lead to radical changes in the conventional model of monetary exchange and we may witness the unbundling of the separate roles of money, meaning that currencies will not only differ in their monetary functions, namely stores of value, exchange media, and units of account, but also the embedded functionalities (Brunnermeier, et al., 2019). CBDCs can provide means to ensure the relevance of public money and retain monetary independence in the future.

Central banks around the world have taken things into their hands with ambitions to develop CBDCs (See Appendix for a state of CBDC by country). Recently, central banks have put digital currencies high on the agenda, given several recent developments in the financial sector. The first of these is the growing attention received by Bitcoin and other cryptocurrencies; the second is the debate on stablecoins; and the third is the entry of big techs into the payment and financial services area (BIS, 2021).

Atlantic Council indicates that there are currently 11 countries with launched CBDCs with the first one being The Bahamas which launched its landmark CBDC called the Sand Dollar in 2020. There are 15 countries with pilot CBDC projects with China becoming the world's first major economy to pilot a digital currency, while countries like Sweden

and South Korea are also piloting their CBDCs. What is important to note, Sweden and South Korea have some of the most established fast payment service (FPS) solutions in the world and both have been witnessing a consistent decline in cash circulation (Duffie, 2019; Bae, 2022). During the interview, Guibourg (2022) notes that while Sweden has been involved with the research and development of CBDC from early on, there is still no decision on definite details of Sweden's CBDC, e-krona, and design. In April 2019, Riksbank sent a proposal to the Swedish parliament to reassess the role of both private and public sectors in the digitalised economy, and consequently, whether Riksbank would be allowed to issue e-krona CBDC (Sveriges Riksbank, 2022). While initially it was expected for the decision to be reached by October 2022, it has been postponed to March 2023. Until then Riksbank will not take any formal decisions in terms of e-krona design (Guibourg, 2022).

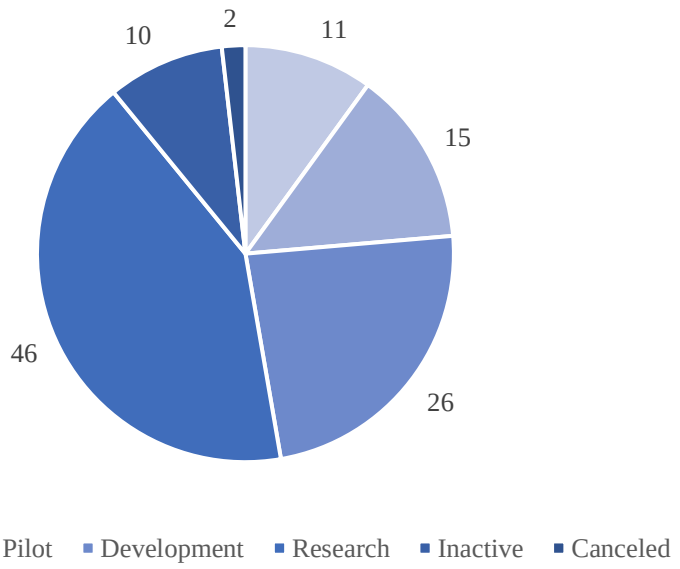

Figure 4: Number of CBDC projects by stage (Atlantic Council, 2022)

The international financial community, academia and other relevant parties are increasingly working towards a common CBDC analytical framework (Morales-Resendiz, et al., 2021) yet the design of a widely accepted and adopted CBDC still remains a question (Ozili, 2022). The impact of the CBDC significantly depends on its design, and in different jurisdictions with different issues and needs, CBDC design might look very different. Thus, implying that there might not be a one-fits-all solution. Morales-Resendiz, et al. (2021) and Ozili (2022) highlight that CBDC requires further

academic research, experimentation and policy discussion. Ozili (2022) points out that the lack of empirical studies is a consequence of CBDC still being in its infancy and lacking real-life applications, as the few countries that have adopted CBDC are still experimenting with this to find the optimal solution. Therefore, it is important to evaluate some of the key characteristics of CBDC to assess which way it can develop further.

1.3.1. Wholesale versus Retail CBDC

Wholesale CBDCs are used by regulated financial institutions for the settlement of interbank transfers and other related wholesale transactions. They build on the current two-tier structure, which places the central bank at the foundation of the payment system while assigning customer-facing activities to payment service providers (PSPs) (BIS, 2021). Central banks already issue digital currencies, in the form of electronic central bank deposits, but these are not for general use in the broad economy. Central bank deposits have generally been limited to banks. Likewise, a central bank could issue cryptocurrency tokens that are restricted for use among a narrow subset of financial firms, and for certain 'wholesale' applications (Duffie, 2019).

Retail CBDCs are described as a 'more far-reaching' innovation (BIS, 2021). Retail CBDCs would make central bank digital money available to the general public, which is not the case currently. In this way, CBDCs, just like cash would be accessible by the general public as a direct claim on the central bank (BIS, 2021). It could also foster modern infrastructures that can reflect the speed, ease of use, and digitally native nature of the new currencies themselves.

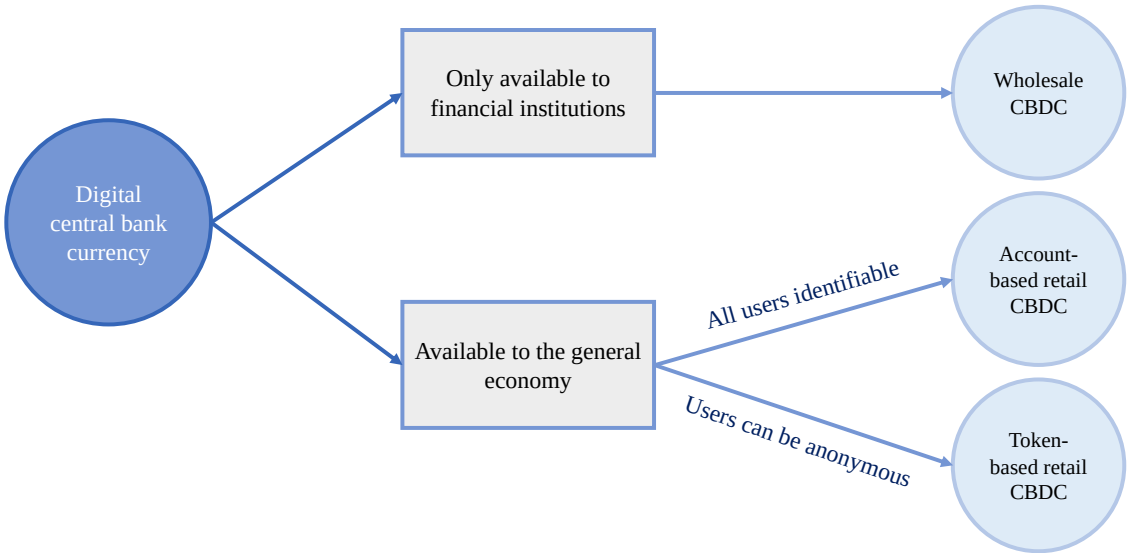

Figure 5: Distinction between wholesale and retail CBDC (BIS, 2021)

With supply chains stretching all over the world, wholesale and retail cross-border payments, the need for rapid and safe payments is only growing. Currently, cross-border transactions face undue friction, long processing times and high fees for consumers. The system involves many parties at play, in this way adding several layers of time, complexity, and expenses to international settlements (Duffie, et al., 2021). While one of the motivations for the wholesale CBDC is cross-border payments, retail CBDC projects are carried out primarily with domestic purposes in mind, at least so far (Soderberg, 2022).

Guibourg (2022) brings three main motivations for AEs to issue retail CBDCs. First, digitization leads to central bank money being marginalised and that means that citizens would lose a choice between public and private money hence driving the financial system to entirely depend on the private sector. The trust system highly depends on an individual being able to exchange private money for central bank money at par at any moment, and if that is lost, the monetary system becomes highly vulnerable. Second, the loss of central bank control could lead to decreased competition, as the system becomes susceptible to monopolies and high barriers for new entrants. Finally, CBDC can increase the robustness of the payments systems and ensure preparation for a crisis or any disturbances that the private system might face (Guibourg, 2022). Meanwhile, EMDEs are, on the opposite, highly dependent on cash and lacking transparency in the system. CBDC can tackle the issue of inefficient distributions, geographical barriers and compliance with KYC, AML, and CFT requirements (Guibourg, 2022). BIS (2021) notes that if a country already has a well-functioning FPS that already efficiently serves the public interest, and data governance and meets all KYC, AML, and CDD requirements, then the benefit that a fully-fledged CBDC could bring less impactful. If, on the other hand, countries that experience significant control exerted by big tech companies and suffer from market fragmentation or lack payment solutions like in many EMDEs, CBDC can bring substantial improvements to the financial system of the jurisdiction. Retail CBDCs are also seen as a potential contingency tool to deploy public resources to households and businesses on a national basis (Morales-Resendiz, et al., 2021). The global pandemic highlighted the importance of distributing economic stimulus rapidly and efficiently, and, in some cases, setting parameters for the use of funds (e.g., supplemental nutrition assistance, housing, or retraining) (Duffie, et al., 2021). Retail CBDC can bring more transparency, safety and robustness to the financial system if implemented well.

	Wholesale CBDC	Retail CBDC
AEs	• Payments efficiency (domestic) • Payments efficiency (cross-border) • Payments safety/robustness	• Payments efficiency (domestic) • Payments safety/robustness • Financial stability
EMDEs	• Payments efficiency (cross-border) • Monetary policy implementation • Financial stability	• Payments efficiency (domestic) • Payments safety/robustness • Financial inclusion

Table 2: Main motivations for issuing retail and wholesale CBDC (BIS, 2021)

The survey data show that central banks are particularly interested in retail CBDCs: all of the BIS interviewed central banks conducting work on CBDCs either look at both wholesale and retail or focus solely on a retail CBDC (Kosse & Mattei, 2022). 43 per cent of the central banks focus solely on retail CBDC, while almost 20 per cent are working on both use cases. Half of all the projects that are already launched, piloting or are being developed solely focus on retail CBDC (Atlantic Council, 2022).

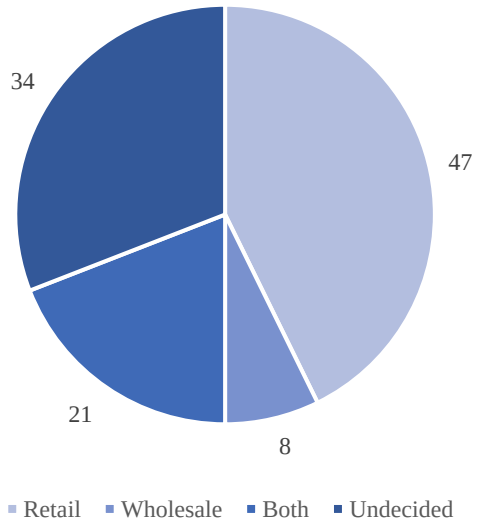

Figure 6: CBDC projects by use case (Atlantic Council, 2022)

1.3.2. Account versus token-based CBDC

One of the key points of the CBDC design is whether it should be account or token-based. Account-based CBDC is a type of CBDC tied to an identification scheme, such that all users need to identify themselves to access it (BIS, 2021). Token-based CBDC is a type of CBDC secured via passwords such as digital signatures that can be accessed anonymously (BIS, 2021). However, as Armelius, et al. (2021) point out, there is a lot of misunderstanding revolving around this discussion and it is somewhat irrelevant, as CBDC cannot be entirely anonymous, offline and peer-to-peer like cash, or equivalently token-based, since all CBDC payments involve a remote ledger that can trace payments history. Duffie, et al. (2021) indicate that the object of paramount importance is the single system of record - the central bank ledger, with a single source of data and the ability for permissioned participants in the CBDC ecosystem to view, access, and act on those data. Critical to this architecture are interoperability capabilities, allowing the different systems of the central bank, commercial banks and other payment service providers to have a common, fully synchronized view of the current state of the central bank ledger. If CBDC tokens are stored remotely, it follows, by definition, that CBDC payments cannot be offline, peer-to-peer or anonymous like cash payments. Armelius, et al. (2021) bring attention to the point that token-based CBDCs could not be stored on local devices and embrace decentralised nature because this raises a double-spending problem, which refers to the ease of illegally copying such tokens. Because of its digital, borderless nature, token-based CBDC which comes with full anonymity could facilitate illegal activity and is, therefore, unlikely to serve the public interest. Even with transaction limits, there is the potential for ‘smurfing’, or laundering the proceeds of illicit transactions into many smaller transactions or accounts (BIS, 2021). Consequently, research has been increasingly supporting the account-based CBDC model with Duffie, et al. (2021) and Armelius, et al. (2021) stating that CBDC, unlike cash, is not a bearer instrument and must ensure that digital payments are between known entities. Bordo & Levin (2017) show that CBDC can become a costless medium of exchange, a secure store of value, and a stable unit of account only if central bank digital currencies are account-based and interest-bearing. BIS (2021) states that identification at some level is hence central in the design of CBDCs, thus, calling for CBDCs to ultimately be tied to digital identity.

One size would not fit all in the choice of digital identification systems, as different societies will have different needs and preferences. For example, during a recent referendum in Switzerland, voters did not object to a digital ID in general, but they

rejected the proposal for one provided by the private sector (Swiss Federal Department of Justice and Police, 2021). On the other hand, in China, the new private entrants have pushed traditional banks to a secondary role. Two private companies, Tencent and Alibaba account for approximately 90 per cent of Chinese mobile payments (Statista, 2022), thus, making society highly dependent on the private sector which gets access to a significant amount of private information. Adrian & Mancini-Griffoli (2019) contemplate that, unlike cash, CBDC would probably not be anonymous, though it could protect users' data from third parties. The question of privacy and security is indeed one of the toughest when it comes to considering an account-based CBDC. As noted by economist Darell Duffie (2021): "The greatest challenge for CBDC designers is protecting the privacy of transactions while at the same time effectively monitoring payments for their legality, particularly with respect to money laundering and financing terrorism." Given the absence of universal data protection laws and the need for better standards and regulatory frameworks in anti-money laundering (AML), countering the financing of terrorism, and the prevention of illicit activity, it is of vital importance to proof the design of an account-based CBDC from any breaches and market arbitrageurs who aim to take advantage of it. Beyond theft, the combination of transaction, geolocation, social media and search data raises concerns about data abuse and even personal safety (BIS, 2021). It is of vital importance for the public sector to ensure that consumers have a meaningful choice when it comes to the privacy of their transactions and control of their data. *Figure 7* shows that privacy and security are key priorities for consumers when it comes to CBDC. However, balancing between the two is a major challenge and may require some trade-offs.

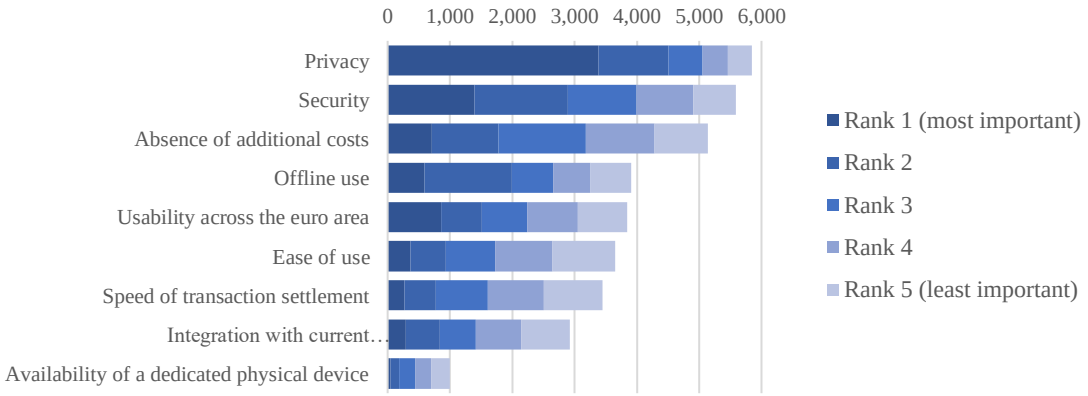

Figure 7: Consumer preferences for central bank cryptocurrency in the EU (European Central Bank, 2021)

1.3.3. One versus two-tier system

As discussed by Auer & Böhme (2020), there are generally two ways in which central banks can distribute a CBDC to the public – either directly (a one-tiered model) or indirectly, via private sector intermediaries (a two-tiered model). In the one-tiered model, the central bank would not only operate the interbank CBDC system but also provide the CBDC account and wallet services directly to the public (Kosse & Mattei, 2022). In the two-tiered model, the central bank and trusted private sector intermediaries would work together (Kosse & Mattei, 2022) with the central bank delegating many operational responsibilities to commercial banks and other payment providers (Duffie, et al., 2021). One problem that arises with a one-tier CBDC system is that central banks would be exposed to a large amount of user data, thus, having to implement KYC, AML, CDD, and CFT processes to ensure the integrity of the users. It would also likely raise concerns from the customers if central banks could see all the transactions a customer makes, and consequently, this might also mean that the government could have access to all the information (World Bank Group, 2021). While in a two-tier system, typical players that comply with these requirements (e.g., commercial banks, PSPs) could continue to interact with the customers, taking this pressure off central banks.

Overall, a two-tiered architecture emerges as the most promising direction for the design of the overall payment system, in which central banks provide the foundations while leaving consumer-facing tasks to the private sector. In such a system, PSPs and commercial banks can maintain their position and continue generating revenue from fees as well as benefiting from an expanded customer base through the provision of CBDC wallets and additional embedded digital services. A CBDC grounded in such a two-tiered system also ensures that commercial banks can maintain their vital function of intermediating funds in the economy (BIS, 2021).

According to a BIS survey, more than 70 per cent of central banks engaged in some form of CBDC work are considering a two-tiered model (Kosse & Mattei, 2022). Activities, where many central banks see a potential role for the private sector, include the onboarding of clients, KYC, AML and CFT processes, as well as the handling of retail payments (Kosse & Mattei, 2022). Meanwhile, the central bank can focus on operating the core of the system to guarantee the stability of value, ensure the elasticity of the aggregate supply of money and oversee the system's overall security (BIS, 2021). Given that the private sector can play a substantial role if the two-tiered model is chosen, most

central banks are considering a retail CBDC architecture that involves the private sector (Kosse & Mattei, 2022). In addition, 76 per cent of central banks working on a retail CBDC are exploring interoperability with existing payment system(s) (Kosse & Mattei, 2022). Consequently, such public-private partnerships could lead to the division of power where central banks would focus on maintaining financial stability, while the private sector could foster innovation.

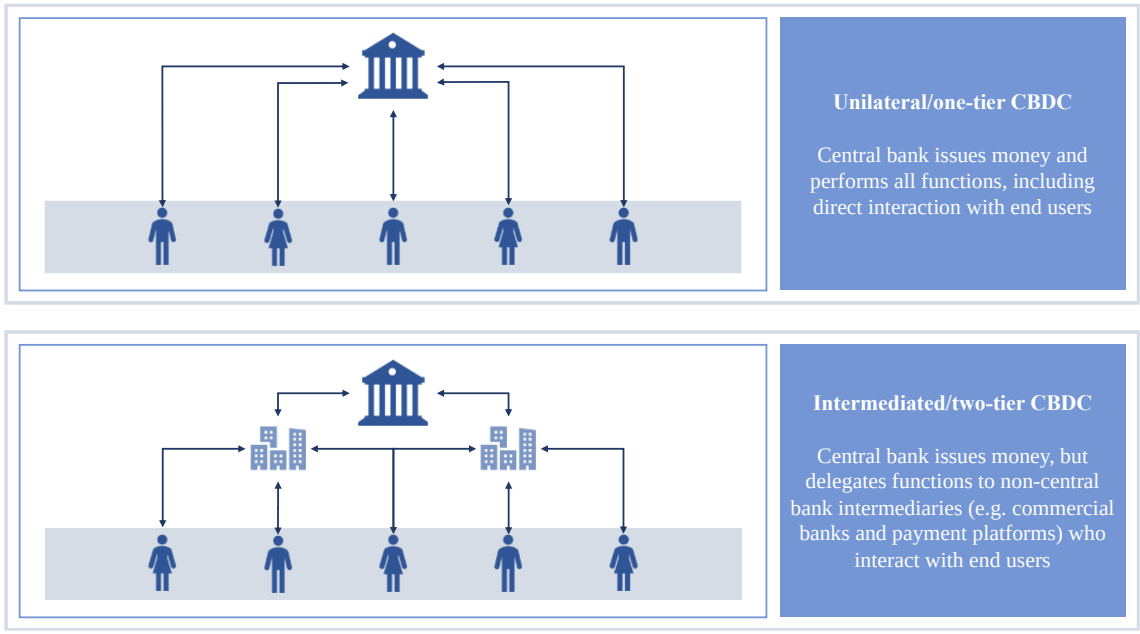

Figure 8: Main conceptual CBDC operating models (Soderberg, 2022)

2. Digital Identity

Just like CBDC, digital identity is still in its infancy. However, Arner, et al. (2018) compare this development with stock exchanges in the 19th century, as "both are set up to reduce the costs of information asymmetries, and both entail a degree of influence on market participants." In the future, the choice of whether or not to have a digital identity will measure up to the question of whether or not to use applications like Facebook or WeChat, as it will become an omnipresent standard in many societies (Zwitter, et al., 2020).

Identity is a fundamental part of the financial sector, and its relevance will only increase with more innovation. Verification of the user's identity, carrying out KYC due diligence and complying with AML, CFT, and CDD requirements are fundamental to market integrity, maintaining trust in the financial system and countering criminal activity (Arner, et al., 2018). Indeed, when the discussion converges to regulatory compliance and security of an account-based CBDC, digital identity emerges as a foundation for it.

While a lot of discussions evolve around technical solutions for digital identity, Zwitter, et al. (2020) request that that identity should first be considered from a philosophical, legal, and ethical perspective. The lack of understanding of a universal concept of identity can lead to an unsustainable and inefficient solution, threatening to bring financial exclusion rather than inclusion.

2.1. What is identity?

The definition of digital identity depends on the eyes of the beholder, as there is no single international standard for the terminology used to describe digital identity (Nyst, et al., 2016). To understand digital identity, it is first relevant to understand our identity in general, and what it encompasses. World Economic Forum (2020) describes identity as defining who a person or organization fundamentally is, namely, a combination of attributes, beliefs, personal/organizational history and behaviour that together constitute a holistic definition of the individual or organizational self. The concept of identity is indeed complex and incorporates both tangible and intangible aspects, thus, making it a major challenge when it comes to precise digital identification of an individual or an organization. Arner, et al. (2018) present an identity matrix that has four core aspects of an identity. First, legal identity is one's legal credentials such as passports, national ID cards or driving licence, and refers to external characteristics of personal information that

summarise who someone is. Second, physical identity refers to elements such as fingerprints IRIS or DNA and refers to internal characteristics. Third, electronic identity is composed of social media accounts such as Twitter, WeChat, Facebook, etc. It is external and not a natural characteristic of a person, yet as people spend more time online, it is becoming increasingly internalized and thus provides a more natural overview and adds to a complete picture of a person. Finally, behavioural identity captures the unique way a person walks, talks and holds their phone and uses various services/products, thus, also referring to the internal characteristics of someone.

	Static identities	Dynamic identities
External characteristics	Legal	Electronic
Internal characteristics	Physical	Behavioural

Figure 9: Matrix of four identity aspects (Arner, et al., 2018)

Identity has been going through an evolution. In the pre-industrial times, with the absence of credentials such as passports and ID cards, people were their reputation. Managing and maintaining reputations among a small social group was not a scalable solution as civilization progressed and moved on to growing trade as the source of prosperity (Birch, 2014). With industrialisation and consequently the emergence of bureaucracy, the definition of identity shifted towards an analogue identity which refers to physical documents and physical markers like fingerprints to record information and establish one's identity. The further development of identity led to digitized identity that relies on the same limited kinds of information as its analogue counterpart but put this information into a digital form, making it more readily available, as our lives have shifted towards a more established online presence with the emergence of the Internet. Birch (2014) states that there is no point in developing an electronic version of "a piece of stamped, security-printed paper with a photo and personal information written on it for inspection." Since an analogue identity is seen as increasingly outdated, the concept of digital identity has been emerging. In this concept, the perception of identity is broadened to include dynamic behavioural characteristics that reflect one's distinct personality, for instance, social media profiles and behavioural patterns can give a number of data points that can give a more defined view of one's personality (Arner, et al., 2018).

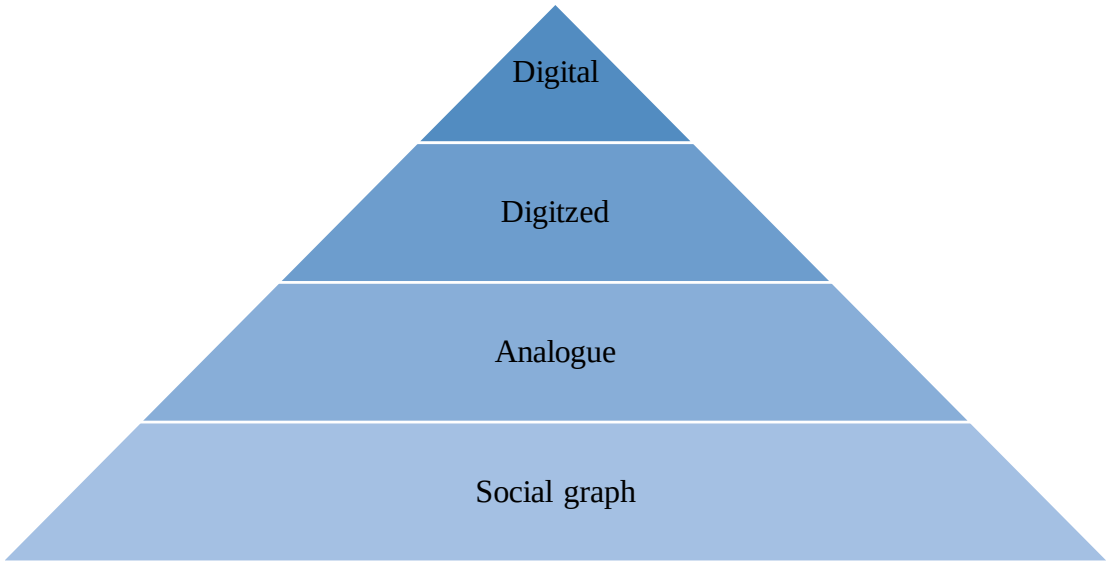

Figure 10: The evolution of digital identity (bottom-up)

When it comes to digital identity, currently, legal and electronic identities play major roles in defining a person in a digital space. Nevertheless, physical attributes that refer to biometrics have become an important part of identifying a person, especially when considering a higher level of identification needed, for example, carrying out financial transactions. Behavioural identification also possesses a lot of potential in the digital space, especially with the emergence of AI and computers' ability to analyse large sets of data and draw conclusions from this. Behavioural identity can add a new layer of security to one's digital identity by analysing how a person interacts with various platforms and identifying any unusual and suspicious actions. While dealing with static aspects of one's identity is fairly easy, electronic and behavioural identities are evolving and changing over time, thus, making it harder to translate them into a digital world effectively. As our lives increasingly shift to digital space, it is important to find a secure and efficient way to translate our identities into a digital world. Arner, et al. (2018) point out that if the definition of an identity dwells only on the aspect of personally identifiable information that mostly concerns legal identity, then the development of digital identities cannot be fully appreciated and dealt with.

2.2. What defines digital identity?

(Zwitter, et al., 2020) points out that while the dimensions of 'classical' human identity have been explored for millennia, the traditional interpretation of digital identity is primarily machine-related. The term digital identity indicates the conversion of human

identities into machine-readable digital data (Masiero & Bailur, 2021). Digital identity can be then described as a digitalized and reduced reflection of what one voluntarily and involuntarily projects into the digital sphere (Zwitter, et al., 2020). While fully reflecting one's identity in the digital sphere can be considered impossible, any identity must have enough attributes to ensure uniqueness, a criterion that derives from the naturalist world view (Zwitter, et al., 2020).

The naturalist view considers everything that resides inside the physical body or is more permanently connected with it, to form one's identity. Thus, implying that everything that is part of or connects to our physical bodies is what makes us unique. Meanwhile, the constructivist view claims that identity is entirely shaped by social structures. Specifically, the relationship with others, the surrounding environment, norms, rules, and institutions are what shape one's identity. Social networks are strong supporters of this stance, as in social media, one's circle (connections, followers, people followed) reflects what a person is. Constructivism in its milder form would at least argue that identity is relational. In other words, who you are is a matter of who you relate to and the nature of this relationship (Zwitter, et al., 2020). Commonly, relationships are registered by governments and expressed through documentation of relational identities such as birth certificates and the entry of someone's marital status into the public record. These relational identity features are affecting the legal status of a person (Zwitter, et al., 2020). But what is also important to note, based on this view, changes in someone's identity influence the identity of another person. This aspect then connects to data ownership, which is one of the key points of discussion when it comes to privacy and security in cyberspace. While data ownership and its disclosure are complicated topics on their own, the fact that data about one person can also be data about another person brings even more complexity to the discussion. This connects to national and international law that require a sufficient level of disclosure about one's legal identity, thus, implying that it is not plausible for an individual to own their data entirely. It becomes apparent that the definition of one's identity lies somewhere in the middle between naturalist and constructivist views. The same applies to data ownership in the socio-legal space, as can be seen in *Figure 11* (Zwitter, et al., 2020).

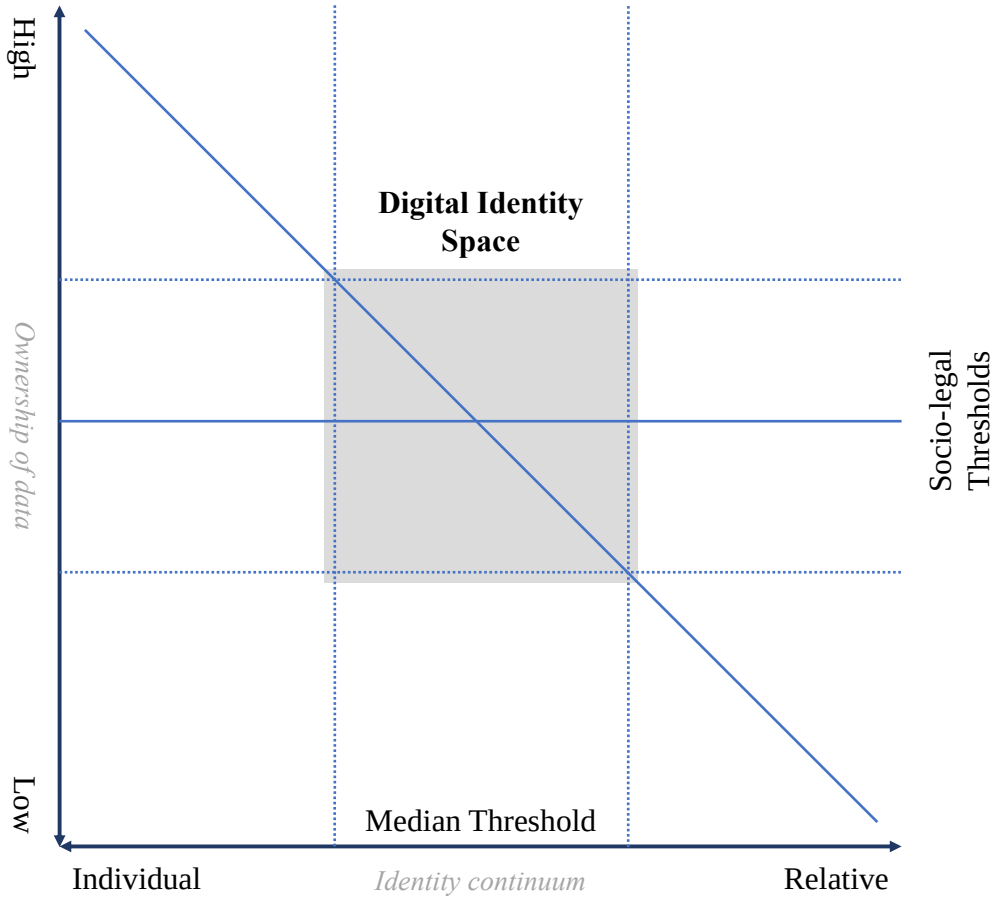

Figure 11: Digital identity space according to (Zwitter, et al., 2020)

Digital identification schemes, as Nyst, et al. (2016) specify, have three functions: identification, authentication, and authorisation, which are all performed digitally. Identification refers to the process of establishing information about an individual. Authentication refers to asserting an identity previously established during identification. The authorisation is determining what actions may be performed or services accessed on the basis of the asserted and authenticated identity (Nyst, et al., 2016), thus, confirming the claims for an individual, for example, an individual 'claiming' to have sufficient funds when making an online payment. All three steps mostly connect to legal and physical forms of identity, as identification usually requires some form of credentials such as a passport, or birth certificate and can also refer to biometric data like fingerprints or IRIS. Both authentication and authorisation then rely on the provided attributes and identifiers to assert one's identity and obtain authorisation for specific actions or services. Goodell & Aste (2019) provide a schematic representation of how typically an identity system works (*Figure 12*). Users first establish a credential with the system (identification), then use the system to verify the credential (authentication), and then use the verified identity

to assert that they are authorised to receive service (authorisation). Besides, Goodell & Aste (2019) also include the fourth function of digital identification schemes – auditing. It refers to the identity system maintaining a record of the establishment, expiration, and revocation of credentials, thus, ensuring that the identity system can explain every successful and failed authentication.

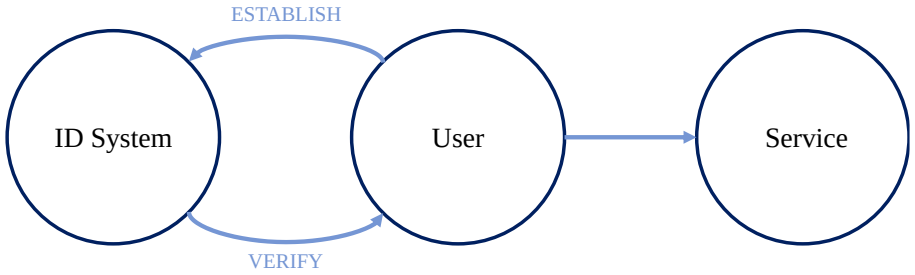

Figure 12: Identity system scheme (Goodell & Aste, 2019)

Klosters (2018) segments identity into physical (tangible) and digital. Physical identity is an enabler of face-to-face transactions and relies on a set of attributes such as a driver's license, passport, device serial number, etc. Meanwhile, digital identity works as an enabler of transactions in the digital world and offers improved functionality for its users. It allows the identification of an entity online/remotely through a set of electronic attributes, namely biometrics, online browsing records and phone numbers. However, Klosters (2018) also points out that the advancements in technology will require a new approach to identity. Indeed, one's physical (or tangible) identity cannot be considered entirely separately from its digital counterpart and the merger between the two is inevitable. Yet it is still unclear to what extent both will converge. If we consider the convergence of our physical and digital identities, it is almost natural to deduct that this digital space, as parallel space to the physical one, does not mirror existing governance structures, power relations, human rights, and legal obligations (Zwitter, et al., 2020).

The device that is instrumental to digital identity is the smartphone which has become a holy grail for participation and expression in the digital age (Zwitter, et al., 2020). At this point, the majority of people have numerous accounts spread out among big tech players on their phones or computers, and this led to siloed identities tied to proprietary services and applications (Verborgh, 2019). Market fragmentation is one of the dangers that digital identity is facing. Without clear standards and regulatory frameworks, digital identity development can take many interpretative forms and instead of facilitating digital

transactions and ensuring privacy and security, evolve into a highly fragmented market that will not only be harder to standardise but also blur the definition of digital identity even more. Without a clear understanding of what digital identity encompasses and relevant related regulations, digital identity can be a source of more problems rather than solutions. Consequently, the essential task of embracing a ubiquitous and widely accepted digital identity is the enforcement of one standard in cyberspace (Zwitter, et al., 2020). While the Internet in general terms has a single technical framework, every day it is experienced through an overwhelming number of kinds of content in at least as many different contexts. The players involved in any one of these contexts aim to take control over digital identity as it can impact their businesses significantly, "in many cases wanting to prevent spillover from their context to any other" (Cameron, 2005). With big techs such as Google, Facebook and Apple, battling over single log-ins, it may hint that the solution might require an extensive contribution from the public sector. While both public and private players play important roles in digital identity development, it comes to an individual who will use that digital identity, and with the lack of trust accompanied by unfavourable conditions and bad user experience, digital identity will inevitably fail. It seems, in the current situation, the emergence of a simplistic and universal digital identity still remains a utopia. What could be a solution though is a network of interoperable digital identities ensuring efficient and reliable operation across borders.

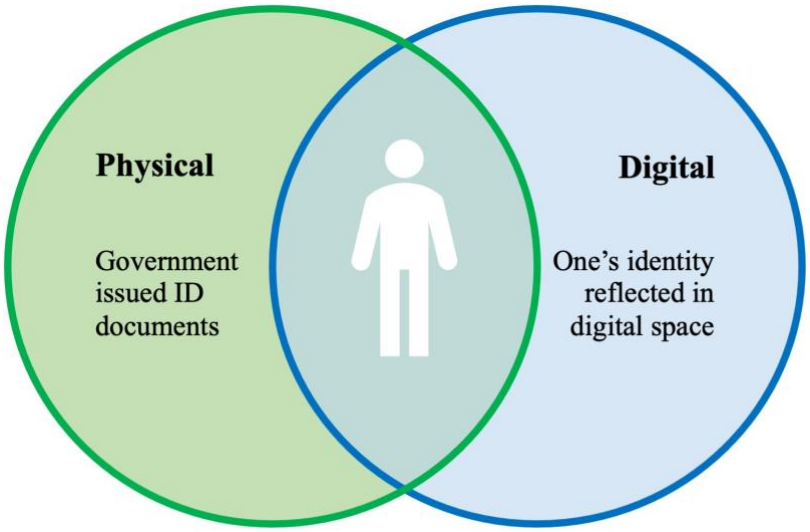

Figure 13: The convergence of physical and digital identities

2.3. Archetypes of digital identity

Know-your-customer (KYC) is a legal requirement for many players in various industries. However, it led to the creation of different onboarding procedures, identification requirements and authentication methods. As KYC and AML regulation requires ensuring the identity of a person that uses specific services, this directly connects to digital identity solutions. World Economic Forum (2018) describes three archetypes of digital identity:

- **Centralised identity systems**: a single either private or public organisation establishes and manages users' identities. Such a system is a s typical set-up between the government and an individual (state keeping records of citizens' data), as well as has become a prevalent model in big tech (e. g. Facebook, Google). For such system to work well, users need to have established trust in the managing party. One of the biggest challenges of centralised systems is the burden that users face with having to handle numerous identities (Zwitter, et al., 2020). Having to remember numerous nicknames, passwords and PIN codes becomes unbearable and centrally storing all the log-in data poses security dangers.
- **Federated identity systems**: different public and private institutions collaborate to establish stand-alone systems and corresponding frameworks. Each institution is bound to the system through agreements and regulations and becomes a trust anchor. This allows re-using identity credentials for several purposes and makes it more convenient for the user. Such a set-up requires an established trust among institutions and a willingness to cooperate. Prominent examples of such solutions are Sweden's BankID, Norway's BankID, and SwissID.
- **Decentralised identity systems**: instead of institutions managing one's identity, the individual becomes in charge of it, while multiple entities 'feed-in' the information about the individual. In such a system, digital identity becomes a resource or an asset as credentials are acquired (World Economic Forum, 2018). Also called 'self-sovereign' identity, it aims to strengthen an individual's position against governments and corporations (Zwitter, et al., 2020). While the decentralised system in theory would tackle the issue of centrally stored information that is susceptible to security breaches, it seems that there has to be a back-up mechanism in case the individual loses or forgets their credentials, for example (Zwitter, et al., 2020). Secure data storage for decentralised identity is one of the key technical challenges that needs to be solved. This system is in its

early stages of development, therefore, it is yet to show whether the expectations will materialize.

System archetypes	Strengths	Challenges
Centralised	• Can be built with a specific purpose in mind; • potential for organizational vetting of identity data.	• Low user control; • centralised risk and liability; • potential for abuse.
Federated	• Users can access a wider range of services; • efficiency for organisations.	• Generally low user control; • high technical and legal complexity.
Decentralised	• Increased user control and a reduced amount of information collected and stored by organizations.	• The governance model, acceptance and participation are complex; • evolving landscape; • complex liability.

Table 3: Strengths and challenges of different digital identity archetypes

2.4. State of digital identity

The blueprint for a European Digital ID began in 2014 when the EU adopted legislation for electronic identification and trust services (eIDAS) among its member countries. Before eIDAS, there were many different national standards for eIDs in member states without any coordination between each other. What eIDAS did is ensure technical interoperability between different technical eID solutions. Instead of creating a pan-European ID card system, eIDAS established a trust-based cross-border solution (Zetzsche, et al., 2019). In 2021, being at the forefront of driving digital identity innovation legislation, European Commission proposed a framework for a European Digital Identity which is set to be available to all EU citizens and businesses (European Commission, 2021a). The framework requires every member state to establish (if not yet done) a national digital ID scheme that then would be linked to the European digital wallet that can be accessed via smartphone or other mobile devices. The users would be able to

upload their national ID documents (e.g. passport, driver's license, professional credentials) onto the wallet and access online services throughout Europe. The European Commission highlights that users would be in full control of their data, as they could share specific information, such as age, without having to reveal other personal details. This hints at the growing tendency towards self-sovereign identity. Besides, digital identity is set to be based on the 'once-only principle' meaning that users don't have to provide the same data twice to public authorities. European Commission has announced a Recommendation to member states (European Commission, 2021b) that is to be followed by a commonly established toolbox that includes the technical architecture, standards and guidelines for best practices. While the toolbox was set to be announced in September 2022 (European Commission, 2021a), the publishing has been delayed given some difficulties evolving in the process.

Indeed, establishing a common ground for digital identity is a difficult challenge, given many member states involved in the process and the potential trade-offs to adhere to strict privacy requirements. The Commission's proposal promises high-level security coupled with convenience and interoperability. Given strict privacy and data protection requirements in compliance with the EU legislation, including the Cybersecurity Act and the General Data Protection Regulation (GDPR) and the complexity of the project, it could potentially require trade-offs to find a balance between different aspects to ensure it can cater for a variety of use cases and meet users' needs.

While an overview of the state in both CBDC and digital identity can be found in an Appendix, *Table 5* provides a list of European countries with an overview of their digital identity solutions. A few selective countries around the globe stand out with their different approaches and experience with developing digital IDs. For example, **South Korea** ranks first in the ability to apply technology in life, business and government with having the most tech-savvy society in the world (Portulans Institute, 2022), and its plan to roll out blockchain-based self-sovereign digital IDs by 2024 (Kim, 2022) will likely put it at the forefront of digital ID innovation. South Korean government seeks new digital ID adoption to reach 45 million people (87% of the population) within 2 years after the launch (Kim, 2022). Given the privacy concerns that stem from a centralised system, the plan outlines that users will store their IDs in their mobile phones and the government will have no access to information stored on individual phones. The system is expected to be entirely decentralised and digital identity will allow individuals to store information such as resident registration numbers, home addresses, bank account numbers, etc.

Mexico, on the other hand, has been developing a centralised biometrics-backed digital ID system. More than 25 organisations have issued a letter to the Senate asking to halt the implementation of the program. They argue that "biometric data is neither the only nor the most effective way to legally identify a person" (Access Now, 2021) and bring concerns over the infringement of human rights and opening the door to authoritarian oversight and security risks for Mexico's citizens. The concerns have a real-life basis, as in 2021, Argentina's government ID database was hacked which resulted in the personal and biometric data of every citizen being stolen and later sold in private circles (Cimpanu, 2021). Kenya and Taiwan have faced similar concerns over their biometric digital ID systems. In 2021, the High Court of Kenya deemed the roll out of the national biometric ID scheme illegal, as it went against the 2019 data protection act (Burt, 2021). In Taiwan, its digital ID implementation was halted until concerns over potential data breaches are cleared out (Yang, 2021). **Singapore** praised its national digital ID system Singpass, which has been quoted as an example of a successful digital ID system that achieved a 97 per cent penetration rate and saved $36 per onboarding (Hersey, 2022). Initially launched 20 years ago as a username and password login for government services, Singpass became an app in 2018 and in 2021 was relaunched on public key infrastructure (PKI) architecture as a cryptography-based mobile app. Singapore has taken an approach of gradually improving products based on lessons learned instead of trying to solve all problems at once. User experience was taken as a key priority to understand what users want and what works best for them, especially among vulnerable users to avoid exclusion. Finally, instead of taking major leaps in adopting breakthrough technology, the relevance of technology and reliance on data sources was thoroughly assessed. **Sweden** is another example of a successful digital ID system implementation and is one of the most mature digital ID systems in the world. Its digital ID scheme BankID was established in 2003 by a consortium of banks in the Nordics and is used in both the private and public sectors. It is one of the few examples of a federated identity scheme, and it has achieved significant success with 95 per cent of the population using mobile BankID, as of 2019 (Wemnell, 2019). It is also an example of how a private digital ID solution can be acknowledged by the public sector and become a ubiquitous solution in the country. Having one of the most mature digital ID systems and piloting its CBDC solution, Sweden is one of the countries with the most potential to lead this innovation. However, recently, Sweden has been criticised for relying on a digital ID that is controlled by a few banks and not having a public digital ID solution (Kinberg Batra, 2022). Kinberg Batra (2022) states that

Sweden, Cyprus, Greece and Romania are currently the only EU countries that lack state digital identification systems. **Turkey** in the meantime has set plans to launch a CBDC that will be integrated with the country's digital ID system and the Central Bank of the Republic of Turkey's FAST instant payments service. Blockchain-based CBDC that is set to be tested for both wholesale and retail payments is planned to launch in 2023 (Börü, 2022).

Country	Name	Year launched	Establisher	Sectors served	Maturity
Sweden	BankID	2003	A consortium of Nordic banks	Public and private	Mature
Norway	BankID	2003	A consortium of Nordic banks	Public and private	Mature
Denmark	MitID (previously NemID)	2010 (new version in 2021)	Danish Digitization Agency	Public, financial services, e-commerce	Mature
Estonia	eID	2002 (new version in 2018)	Government	Public and private	Mature
Belgium	itsme	2017	A private consortium of seven banks and mobile operators	Public and private	Mature
Finland	Electronic ID	2004 (new to come in 2023)	Government	Public	Active
Netherlands	DigiD	2003	Government	Public	Active
Ireland	MyGovID	2017	Government	Public	Active
Germany	Digital ID	2017 via PC and since 2021 for mobile phone	Government	Public	Active
France	FranceConnect	2016	Government	Public	Active
Italy	SPID	2016	Government	Public	Active
Portugal	Cartão de Cidadão	2007	Government	Public	Active
Czech Republic	mojeID	2010 (hardware token, later	Government	Public	Active

		supplemented by mobile app)			
	eDokladovka	To be launched in 2023 (ID wallet app)	Government	Public and private	Active
Austria	Mobile driving license	2021	Government	Public	Partly active
Spain	Electronic ID card	2006	Government	Public and private	Partly active
Slovakia	Electronic ID card	2013	Government	Public and private	Partly active
Hungary	Digital ID card	2016	Government	Public and private	Partly active
Slovenia	Digital ID card	2022	Government	Public and private	Partly active
Croatia	Electronic ID card	2013 (new version in 2021)	Government	Public and private	Partly active

Table 4: An overview of digital identity in European countries (Fitri, 2022)

2.5. Reimagining digital identity

When talking about the future development of digital identity, Arner, et al. (2018) raises three main concerns: 1) electronic identifier can be tampered with/faked; 2) loss of privacy; 3) monopolization and the risk of abuse from market power. Privacy has been an important participant in digital identity discussions, conflicting with another crucial aspect – security. Privacy is often seen as an obstacle to technological development, and it is often considered that in order to achieve good user experience, convenience, efficiency, technical interoperability, and viable commercial business models, privacy trade-off may not be avoided. However, "privacy is set to enable rather than restrain" (Nyst, et al., 2016). Privacy is a fundamental human right, allowing individuals to develop autonomously and take control over their decisions. Privacy plays a functional role in any democratic society, with a great example of it being the EU which has established extensive privacy laws (e.g., GDPR). The right to privacy has evolved to embrace a right to data protection, thus, meaning that individuals can control who has data about them and what decisions are made on the basis of that data (Nyst, et al., 2016). However, as can be observed in the current system, individuals often lose control over their data or are not even aware of what personal information of theirs is available or held by other parties. The most prominent example of this is big tech (e.g., Facebook), where users' data is used for commercial purposes and users face major obstacles to obtain full disclosure of what

kind of personal data is held by big techs. As the matter of trust is concerned, BIS (2021) study identifies that incumbent financial institutions are the most trusted parties in handling user data properly. Interestingly, customers have the same level of trust in fin techs and government agencies, while big techs are least trusted among all.

2.5.1. Decentralised identity

Decentralised identity is seen as a way to bring control back to users. The management of digital identity is transforming "from a purpose-driven necessity toward a self-standing activity that becomes a resource for many digital applications" (Zwitter, et al., 2020). While traditional identity solutions were primarily focused on specific sectors or services, digital identity management is transforming into a basic infrastructural service, sometimes even a commodity (Zwitter, et al., 2020). This coincides with the concept of decentralised identity that aims to give users the ability to manage their digital identities autonomously. As mentioned before, decentralised identity is a new concept that succeeds centralised and federated identity archetypes. The term 'decentralised identity' is used interchangeably with 'self-sovereign identity' and currently, there is no universal and legally binding definition of a concept, yet it is clear that its main focus is about putting the user at the centre of identity management. Wagner, et al. (2018) have proposed to define self-sovereign identity as "a model of digital identity where individuals and entities alike are in full control over central aspects of their digital identity, including their underlying encryption keys; creation, registration, and use of their decentralized identifiers [...] The architecture gives individuals and entities the power to directly control and manage their digital identity without the need to rely on external authorities." The technology that is mostly referred to as a way to enable decentralised identity is distributed ledger technology (DLT). While digital identity management frameworks are not exclusively discussed as built on DLT, such technology can enrich the governance toolkit and be a part of useful solutions "but only if it can incorporate socio-legal and philosophical necessities that digital identity brings with it" (Zwitter, et al., 2020). There are still many unknowns revolving around DLT that concern privacy, efficiency, scalability, etc. But if the right solution is found and it can be well translated into practice, DLT has the potential to strengthen individuals' rights and improve their experience. The CBDC proof of concept tested by the European System of Central Banks (ESCB) has shown that in the simplified environment DLT can be used to balance an individual's right to privacy with the public's interest in the enforcement of AML/CFT regulations

(European Central Bank, 2019). However, it also led to the conclusion that the information visible to parties not involved in the transaction must be reduced to ensure integrity. In the proof of concept, intermediaries validating a CBDC transaction had to look at the information on past transactions of the CBDC units being transferred, all the way back to the moment when they were first issued (European Central Bank, 2019). It is unclear how the existing law on financial confidentiality and data protection for personal data relates to DLT technology (Sveriges Riksbank, 2022) and this may hinder the wide adoption of this technology. When speaking about CBDCs, Guibourg (2022) also mentioned that policy rather than technology is leading the way which also applies to digital identity as both are considered to be adopted on DLT infrastructure. Thus, the implementation of DLT substantially depends on whether it can adhere to regulatory requirements.

2.5.2. Unitary identity versus multiple identities

Ensuring user-friendly design and adhering to cultural norms is crucial for the mass adoption of a new concept of digital identity. Users will not be willing to use something that they do not grasp easily and that requires more effort than existing solutions. Thus, it raises a major challenge, since self-sovereign identity is all about users being in control of their identities and the data they share. Nevertheless, such technology may come with specific complexity in user experience and thus raising obstacles for mass adoption such as lack of understanding of how it works, complex onboarding and maintenance of one's identity, etc. One potential solution could be a 'master key' that allows each user to prove that all of their credentials are related to each other via a unitary avatar (*Figure 14*), as proposed by Camenisch & Lysyanskaya (2001). However, Goodell & Aste (2019) take issue with the approach that an individual would have no more than one identity, claiming that while unified identity can serve in terms of convenience, the "potential for blacklisting and surveillance that early-binding introduces is significant". Besides, Goodell & Aste (2019) also claim that systems that encourage individuals to establish unitary identities for use in various contexts can ultimately influence and constrain how such people behave. When people are aware of being watched, they alter their behaviour. This is known as the Hawthorne effect (Spencer & Mahtani, 2017). This relates to one's restricted ability to entirely reflect their personality, thus, also leading to potentially unnatural choices and actions.

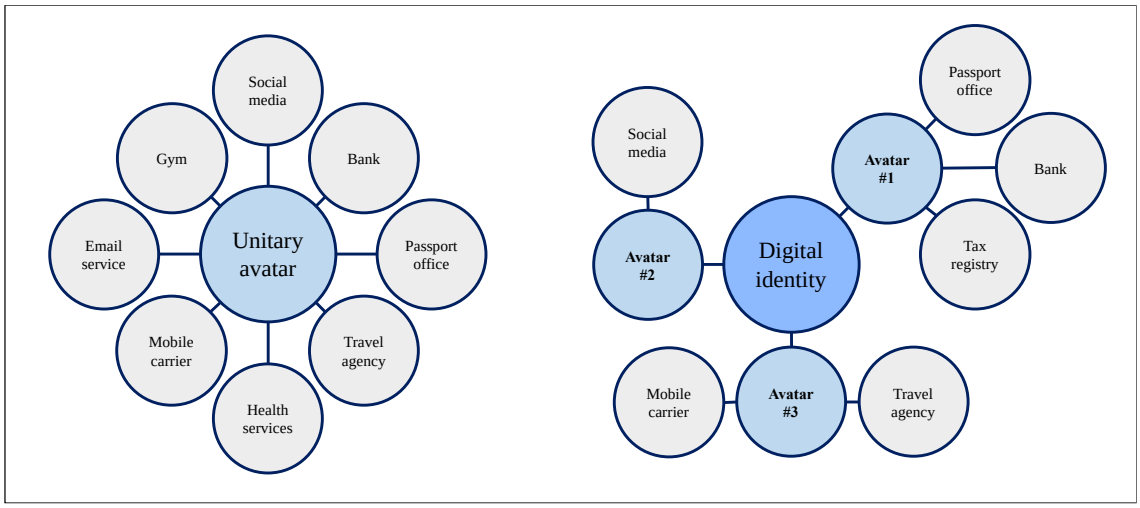

Figure 14: Unitary identity versus multiple identities with different levels of disclosure (Goodell & Aste, 2019; Birch, 2014; The World Group, 2018)

In the context of physical documents, generally, people have multiple identity documents already and even though they all refer to one person, they usually are used stand-alone and need not be presented as part of a bundled set with explicit links between the attributes (Goodell & Aste, 2019). This can be reflected in the digital space with an individual having several avatars that disclose different levels of information about the person, as can be seen in *Figure 14*. As different platforms and spaces require different levels of information about one's identity, this could minimise the need for unnecessary disclosure of information.

One question that arises when considering multiple identities versus unitary identities is the level of disclosure. For example, when a person is buying alcohol at the store, the cashier does not need to know their name, surname, etc. All that matters is whether the person is of legal age to buy it. Thus, the future of identity could enable users to show that they are entitled to specific services or products and avoid disclosing any irrelevant information. This is extremely relevant for a digital space. Birch (2014) discusses the privacy paradox that states "in order to harness the power of the Internet, we want full disclosure from everybody else who wants to be part of the subgroup but will refuse any kind of disclosure on our side." Indeed, the ability to exchange relevant data without disclosure of our identities could make the Internet a significantly safer space. Wagner, et al. (2018) describe Zero Knowledge Proofs (ZKP) which is a feature of DLT and could serve in this case. Wagner, et al. (2018) present it in a way that "allows two different actors, the "prover" and the "verifier" to exchange the ownership of a piece of data, without actually revealing the data." This relates to claim-based identification where an

individual does not disclose their identity to gain access to services and products but instead shows that they are entitled to it. Birch (2014) discusses token-based identity which is based on 'tokens' that refer to claims allowing people to access specific services without disclosing personal information. It does not relate to the definition of token-based CBDC given that it could not function entirely anonymously, as in the idealised case of a token-based CBDC. Individuals could hold claims, for example, in the form of tokens in their digital wallets that ensure their entitlement such as driver's license, being above 18-year-old, picking up deliveries, booking hotels, writing reviews, etc. To discuss the latter, it has become common knowledge that many reviews tend to be fake and are easy to fabricate. With a claim-based identity, for instance, after staying in a hotel, individuals would get a special token that would ensure their claim to write a review, in this way, ensuring the authenticity of reviews (Birch, 2014). Claim-based identity could facilitate transactions in a broad digital space. Besides, witness protection is another example where it could replace purely biometric and centralised solutions which can fail to protect individuals under the witness protection scheme. Individuals' privacy can potentially be protected by shifting from centralised to decentralised cryptographic techniques. DLT holds a lot of potential when it comes to the digital identity of the future, yet it needs to find the balance between anonymity and transparency. DLT boasts that it can provide full transparency and immutability to all transactions and bring a new level of trust. While on the one hand, it can bring substantial benefits, on the other hand, this transparency and immutability stand against data disclosure regulations, for example, a person's entitlement to be forgotten under Article 17 of the EU GDPR (European Union, 2016). Coming back to the disclosure of information that only is relevant to specific situations, it is important to consider anonymity and to what extent it is acceptable.

2.5.3. Anonymity versus transparency

Arner, et al. (2018) highlight that 'anonymity is a feature, not a failing, of the internet.' The possibility and acceptability of anonymity and the use of avatars and nicknames as one's way of identity have contributed to the success of numerous Internet businesses (Arner, et al., 2018). While acceptable in some cases like in social media, anonymity is neither universally compatible nor acceptable for many purposes (e.g. when it comes to online payments). Cryptocurrencies could provide total anonymity, not requiring any means of identification for transactions, and consequently, they emerged as a way for financing criminal activity, money laundering, etc. Anonymity relates to individuals'

rights to have free will and act upon it. The anonymity discussion is a difficult one because there is little consensus in national and international laws as to what scope individuals have the right to remain anonymous. Countries such as the US and EU member states have strong privacy laws and ensure the right to anonymity. For example, the Committee of Ministers of the Council of Europe adopted a Declaration on freedom of communication on the Internet which establishes anonymity as a central principle of freedom of communication, declaring that "in order to ensure protection against online surveillance and to enhance the free expression of information and ideas, member states should respect the will of users of the Internet not to disclose their identity" (Organization for Security and Co-operation in Europe, 2003). Meanwhile, in Brazil, for example, the Constitution allows freedom of expression, but it cannot be anonymous (Reuters, 2017). Anonymity is very important for people in marginalised and oppressed groups as well as living in authoritarian countries, as it can allow them to not only communicate about the issues, they face but also protect them from life-threatening consequences. Therefore, it must be considered how people can have the peace of mind to act upon their free will while also being sure that they are not being put under surveillance.

World Economic Forum (2018) imagines the future of digital identity as one system connecting our every online/offline interaction, being linked to:

- Every click, comment, and share one makes on social media;
- Every financial transaction one records;
- One's location and where one travels;
- What one buys and sells;
- One's personal health data and medical records;
- The websites that one visits;
- One's participation in civic functions (i.e., voting, taxes, benefits, etc.);
- How much energy one consumes;
- One's carbon footprint.

And that is not an exhaustive list. "This digital identity determines what products, services and information we can access – or, conversely, what is closed off to us," according to the same World Economic Forum (2018) report. Such a vision can be seen as quite complicated and problematic for reasons mentioned before, namely freedom of choice and actions, privacy, and human rights. Neither total anonymity nor too much transparency is optimal. Instead, transactions should be private with the focus shifting towards pseudonymity, allowing people to engage in economic and social transactions

without having to give away too much information about themselves in the process. Yet, for pseudonymous identities to function well and be trusted, they have to be underwritten by institutions that generally have a high level of trust (Birch, 2014). Referring to *Figure 1*4, Birch (2014) suggests that a very practical way for people to take control of their interactions is by establishing multiple personas/avatars formed by pseudonyms. Each avatar could have different levels of disclosure and could be reused for relevant institutions and platforms. The previously mentioned CBDC proof of concept of the ESCB has suggested enhancing privacy using mechanisms such as rotating public keys, previously mentioned zero-knowledge proof and enclave computing (European Central Bank, 2019). Rotating keys, for example, refer to users generating pseudonyms regularly, in this way, limiting nodes' ability to link transactions to individual users, as users would be using various different pseudonyms over time. At the same time though, intermediaries would still be aware of all the transactions initiated and received by their respective clients, and the AML authority would know the real identities of the payer and the payee whenever transactions without anonymity vouchers were sent for approval (European Central Bank, 2019). While this proof of concept was carried out with CBDC in mind, a similar logic can be applied in developing a decentralised digital identity.

2.5.4. The value of data

World Economic Forum's (2018) vision of digital identity encompasses the majority of aspects of one's life. With all this data, digital identity can become a tool for various institutions, especially financial ones, to assess users' risk profiles. Fin techs already capture both behavioural and financial data to create a better image of the user. Payment platforms, for instance, are perfectly positioned to gather large amounts of users' data and work as an ideal predictive tool for users' preferences and behaviour (Brunnermeier, et al., 2019). There are numerous behavioural aspects that extend beyond financial tendencies to gain a better understanding of a user and in this way personalize their experience and offering. First, physical behaviour like the way a person holds their phone or enters their password can contribute to improved authentication and can act as a second-factor authentication method (Arner, et al., 2018). Second, behavioural tendencies like time spent on websites, shopping habits and hobbies can provide a lot of insight into one's persona, and consequently, evaluate certain risks in better detail. This can help financial institutions like credit or insurance companies to innovate their processes. Having this information embedded in one's identity can allow personalized services and

financial offering that is based on more accurate risk profile evaluation. As mentioned before, World Economic Forum (2018) envisions that even one's carbon footprint could be connected to their identity and in this way, individuals could, for example, pay a premium or even be denied buying flight tickets if their carbon footprint exceeds the norm. While such an approach can innovate the sphere and bring more assurance, this can be seen as highly problematic and clash with basic human rights.

Arner, et al. (2018) submit that for the forward-looking digital identity framework, it is crucial to consider three separate issues: digital identity, data management and financial regulation. Data can be a key variable in redefining how digital identity interacts with various services, creating a united ecosystem that eliminates redundancy by making every step necessary for client onboarding and back-up checks to be carried out simultaneously, and only once per client for all kinds of services and intermediaries. This would mean embracing a sector-wide KYC system where many players interact with each other and feed information into the user's digital identity, making it easier for the user to manage it while also bringing more transparency and reducing risk. Arner, et al. (2018) provide an example of such a system, where a range of KYC information is embedded into one's identity: "These identifiers could include information on links to exposed political persons (1 = yes, 0 = no, plus country identifier) and the range of financial services deemed suitable for the entity (10 = all, 9 = complex derivatives to 0 = state bonds only). This data would be machine readable and determine which client relationships would be subject to additional checks. Once established, the receiving financial institution would tap into the KYC utility only to check whether new information is available; and these types of checks could also be fully automated, superseding manual processes. The information embedded in the transaction code will not always be collected by the same entity. For instance, the payment service provider that accepts the client's money for the first time within a jurisdiction may review the AML questions, while the first investment firm selling the client investment products may add information on suitability. As accountability is vital, records of who has added which information and when are essential, which, once again, suggests some form of blockchain system as a potentially suitable underlying architecture." While all institutions collaborating to feed into one's identity may sound unlikely and even utopian, this step can accelerate the development of digital identity significantly. Interoperability is identified as one of the key requirements for a well-functioning cross-border and cross-sector digital identity that is seen as the future. It can already be observed by big tech companies allowing to transfer

account details from one platform to another. For example, one can use their Google credentials to log-in to LinkedIn which is owned by Microsoft. Yet the fight among big techs for control over users' identity is very apparent, thus, negatively affecting willingness to cooperate, and hence interoperability. While it may not be easy to trust an individual from the first point of view, institutions tend to have a sufficient level of trust established among each other, thus, one institution could confirm the identity of an individual for another institution. For example, instead of having to close a bank account at one bank and then go through all the steps to confirm one's identity when opening an account at another bank, an individual's information could just be transferred directly without having to repeat all the KYC checks. Besides, existing customers of financial institutions such as banks often find it difficult to open a bank account with the same institution in another country which could be fairly easily fixed (Klosters, 2018).

Custodianship of digital identity is an important concern that arises when discussing digital identity design solutions. The arguments are raised that ownership of information should be in the hands of users, rather than with whatever entity is collecting the information (Arner, et al., 2018). A system that does not put users in control will – immediately or over time - be rejected by enough of them that it cannot become and remain a unifying technology (Cameron, 2005). Yet, there have to be institutions that provide infrastructure and maintenance, either public or private, or both. While public institutions are seen as the ones responsible for legal frameworks and pushing the agenda further, private parties are seen as the ones capable of real innovation. However, the question is what private parties that are profit-driven can take from this. Identity transactions do not involve a direct flow of money and so, unlike payments, there is no opportunity to take a slice of the transaction value (Nyst, et al., 2016). Besides, for a consumer, an identity scheme is only of interest if it is accepted by a wide variety of service providers. For a service provider, an identity scheme is only of interest if it is used by a significant proportion of the service provider's customers. Therefore, both conditions need to be satisfied simultaneously (Nyst, et al., 2016). This brings back the interoperability question and what institutions stand to gain or lose in building a next-generation digital identity scheme.

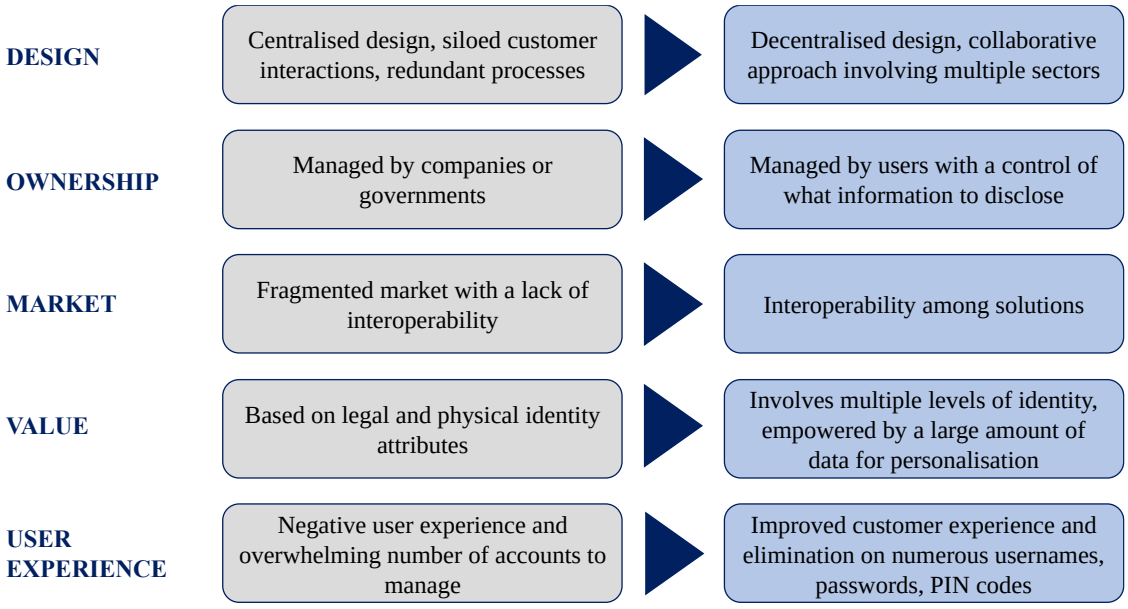

Figure 15: The shifting concept of digital identity

3. CBDC and digital identity

3.1. The connection between CBDC and digital identity

Based on the research that has been carried out, *Figure 16* summarises the general trajectory towards which CBDC development is leaning. First, retail CBDC can tackle significant issues that both AEs and EMDEs are facing and bring impactful innovation to the financial system. CBDC cannot be entirely anonymous given the traceability of digital payments and the need to tackle financial crime, thus, account-based CBDC seems like the most likely and logical course of direction. Finally, a one-tier system would put major pressure on central banks that would have to take over many operational tasks with one of the most challenging ones being the management of users' data. A two-tier solution hence can help central banks to avoid this hurdle and maintain the current position of other players like commercial banks and PSPs. By any means, this is not a definitive direction of CBDC design choices, as different needs (e.g., varying motivations for AEs and EMDEs) can lead to different design choices. However, a unitary standard could help to avoid fragmentation and alleviate cross-border interoperability. CBDCs have gained significant attention over the past years, and their development has in general been accelerating. Yet the majority of central banks and governments have been careful in making definite choices and we are yet to witness how this will develop in the future.

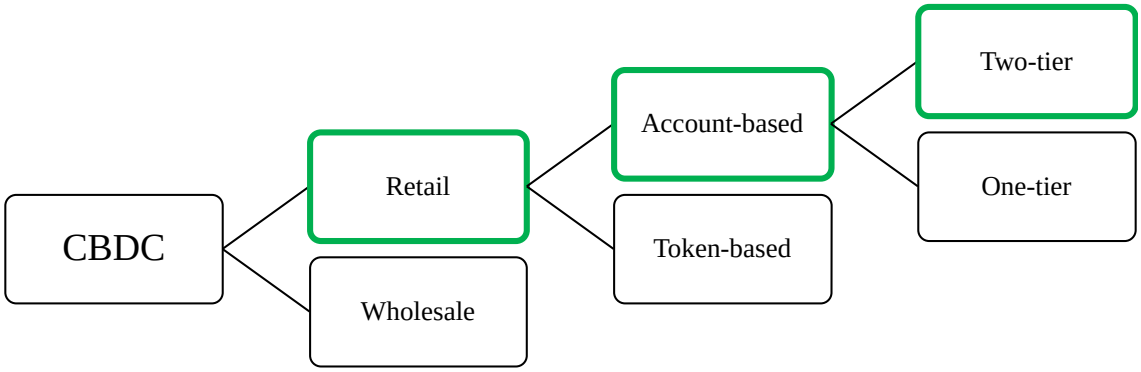

Figure 16: The summarised trajectory of CBDC design choices

Digital identity, on the other hand, while extremely relevant in the digital age, has been developing fairly slowly. While the emergence of DLT technology can lead to major breakthroughs in the digital ID space, to quote Guibourg (2022) again, "policy leads the

way, not technology". Assessing the relevance and efficiency of technology is instrumental in establishing the right policies that will define the development of digital identities, but we are yet to see it. As for CBDC, *Figure 17* depicts some of the key characteristics that are likely to build a foundation for the future of digital identity. Centralised systems are susceptible to major privacy breaches and one institution in charge of large amounts of data is seen as an outdated model that puts users at disadvantage. Even though surrounded by many questions decentralised system can bring significant innovations and adapt digital identity to our increasingly digital lives. The EU and South Korea are already working on building next-generation digital IDs based on this model. While having a unitary avatar that can be used for interacting with every service might be convenient, it can be seen as problematic, since it would lead to a lot of unnecessary data disclosure. Digital identity divided into several avatars/IDs, each with a different level of disclosure can provide a balance between privacy and convenience. Finally, either full anonymity or full transparency are not feasible. Instead, pseudonymity can be the solution that can allow secure identification coupled with the maintained privacy of users. Currently, digital identity seems to revolve around biometrics and centralised solutions, yet as the practice has shown, such technologies can pose danger to the privacy and security of the users. While the first attempts at a universal identity system are being made, the reality remains that the individual is composed of a patchwork of identities, logins, usernames, passwords, etc. (Zwitter, et al., 2020).

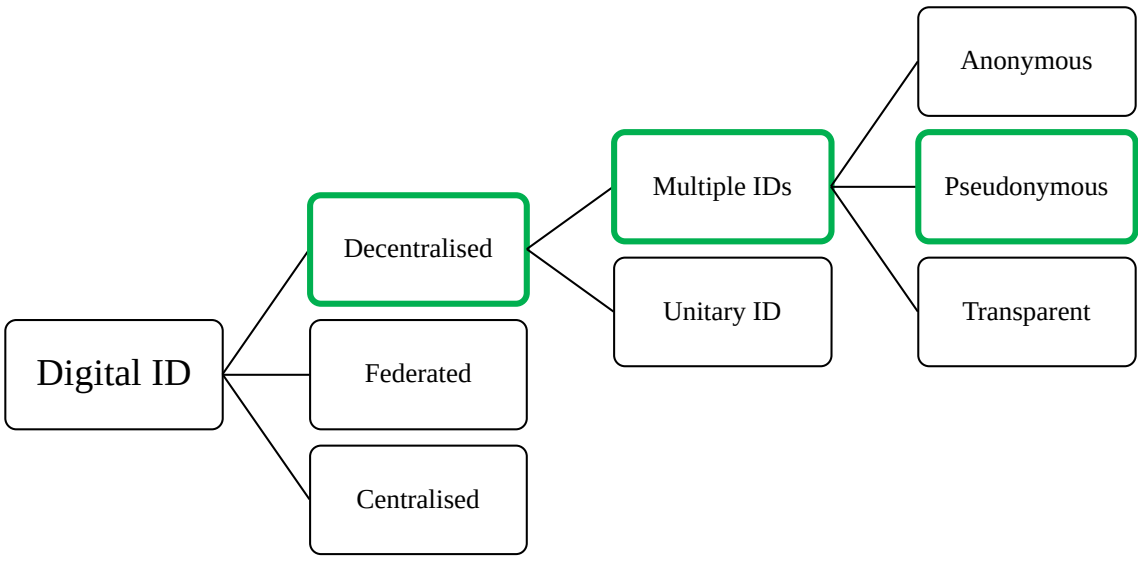

Figure 17: The summarised trajectory of digital identity development

One thing that is clear, digital identity has an important role to play in the roll-out of account-based CBDCs. Yet as both have many complexities in their design, finding the best way for them to interact with each other is a major challenge. Given that countries are driven by varying motivations, it might be especially challenging to establish unifying standards that would allow cross-border efficiency and security. Mobile phones have been a key instrument in driving the ongoing digitization, and they are critical in both CBDC and digital identity. Retail CBDCs would be kept in digital wallets, while the same can apply to digital identity. The question is whether both could be combined to be placed in the same digital wallet, and how would that work. Since an account-based CBDC is set to have an identity layer, and both are discussed to be based on DLT, the right design could bring the simplicity of managing one's identity and money. Both identity and money are changing profoundly, and Birch (2014) suggests that as those two trends are converging, all we will need for transacting in the future will be our identities. If we consider that cash in circulation is declining and might eventually be overtaken by CBDCs that will be connected to digital identities, this suggestion is likely to hold true. Brunnermeier, et al. (2019) and Birch (2014) submit that we will go beyond multiple national currencies and will eventually have different kinds of money that serve different purposes (cash and non-cash transactions). We might witness the unbundling of the roles of money, where money does not have to be a store of value, medium of exchange, and unit of account simultaneously. Instead, with the falling switching costs, different currencies can serve different purposes and transcend national borders to thrive in the borderless digital space. In a digital economy with such systems where most activity is conducted via networks, it is a must to ensure that all money is convertible to CBDC which would maintain the unit of account status of public money (Brunnermeier, et al., 2019). However, while private money might to some extent uphold anonymity, CBDC will require a trustworthy identification system, thus, it is unclear how interoperability between currencies in such cases would work. Interoperability between platforms and CBDC is essential for the success of both private and public digital money to ensure that publicly issued CBDC is sufficiently attractive to the general public while also providing the anchor for private money (Brunnermeier & Niepelt, 2019). Interoperability across borders and platforms should be one of the key considerations for policymakers to avoid fragmentation and excessive barriers across borders. Ensuring interoperability can also have a significant impact in the digital identity space, as the current systems are hampered by inefficiencies and costly manual KYC processes that are often conducted multiple

times as financial institutions are not designed to 'trust' each other and their data (Klosters, 2018). Building a digital identity that can ensure trust among different players can help to eliminate repetition and achieve significant cost savings.

Our financial system is moving from one based on KYC principles to one based on a Know-Your-Data approach (Arner, et al., 2016). Data embedded in one's identity can reflect on CBDCs and thus not only provide a personalised experience but also put financial constraints, for example, interest rate tiering depending on household-specific holdings or caps on holdings altogether (BIS, 2021). This is crucial to consider in the regulatory paradigm, as there is a thin line between ensuring more efficiency and infringing human rights by imposing excessive control on one's choices.

Privacy is one of the key concerns in digital identity and CBDC, and as Guibourg (2022) mentioned, privacy does not mean anonymity. While anonymity is important to protect the free will of people, it is clear that full anonymity is impossible. Instead, the design choices have to find a way to protect users' integrity while simultaneously ensuring the safety of the financial system. Currently, very often we have to disclose unnecessary information to prove our claims. The future of CBDC and digital identity has the potential to eliminate this. Self-sovereign identity could potentially suggest a solution in this case, as the data is to be managed by the user who could selectively share the needed information and control over their credentials. This falls in line with the fact that central banks should not know everything about the customer (nor do they want to in most cases) and restrict the disclosure of information to only knowing enough to keep the system working in a secure way. Indeed, the concentration of data in the hands of a single institution threatens legal safeguards for data protection, consequently, making self-sovereign identity a potential solution to this issue. Yet we seem still far from the practical application of self-sovereign identity, even though South Korea and the EU are making major strides in its implementation. As countries are working on an account-based CBDC design, it remains unclear who and how should verify the identity of an individual seeking to join the network of CBDC users. While digital ID schemes are emerging, their specific designs and roles differ substantially, making it difficult to establish any kind of standards for safe identification in the CBDC space.

With the development of CBDCs and digital identity, we can expect the emergence of new business models that can foster innovation. However, Guibourg (2022) mentioned that potential business models still need to be analysed further, as it is currently still unclear what incentives there will be for the private parties to contribute to the CBDC-

driven goals. Some sectors such as fin techs might be motivated to gain easier access to the payments systems, or merchants might seek to reduce the costs of the payments system that they have to bear now (Guibourg, 2022). The fact is that for private parties to be involved in the development of both CBDC and digital ID development, they need to see a clear source of revenue. In the example of digital ID, identity transactions do not carry any transaction costs, thus, private parties cannot shed a part of them. Incumbent financial institutions are one of the very few types of institutions that can verify user information and have a fairly high level of trust within society. However, their motivation to innovate might be limited. Current players might be incentivized to jump on the CBDC and digital ID development bandwagon not to lose their competitive position in the market though. It is the role of policymakers to ensure that they foster innovation and promote new business models that can solve some of the key CBDC and digital identity design challenges. Therefore, it ideally can create opportunities for new players to enter the market and in this way foster competition.

Rethinking and implementing new CBDC and digital ID approaches can have a substantial impact in emerging markets, as many people face financial exclusion being incapable to provide a valid ID document. Creating a digital twin of one's physical identity (or in some cases, making digital identity the central form of identification) can open many opportunities for vulnerable groups, but it must be considered that digital identity can also be a tool for exclusion and such actions must be prevented in its design.

3.2. Principles for digital identification and CBDC

World Bank Group (2018) sets Principles on Identification for Sustainable Development (*Table 5*). Providing "legal identity for all" by 2030 is now Target 16.9 under the Sustainable Development Goals (SDGs). It is also increasingly seen as instrumental to achieving many other development goals and targets.

Inclusion: Universal coverage and accessibility	Ensuring universal coverage for individuals from birth to death, free from discrimination.
	Removing barriers to access and usage and disparities in the availability of information and technology.
	Establishing a robust-unique, secure, and accurate identity.

Design: Robust, Secure, Responsible and Sustainable	Creating a platform that is interoperable and responsive to the needs of various users.
	Using open standards and ensuring vendor and technology neutrality.
	Protecting user privacy and control through system design.
	Planning for financial and operational sustainability without compromising accessibility.
Governance: Building Trust by Protecting Privacy and User Rights	Safeguarding data privacy, security, and user rights through a comprehensive legal and regulatory framework.
	Establishing clear institutional mandates and accountability.
	Enforcing legal and trust frameworks through independent oversight and adjudication of grievances.

Table 5: Principles on Identification for Sustainable Development (World Bank Group, 2018)

G7 (2021) has also set Public Policy Principles for Retail Central Bank Digital Currencies (*Table 6*). It encompasses a variety of crucial matters that have to be reflected in the design of CBDC. What can be observed, is that World Bank Group (2018) principles on identification and G7 (2021) principles on retail CBDC share many aspects.

Foundational issues	
1. Monetary and financial stability	Fulfilment of public policy objectives and preventing harm to monetary and financial stability.
2. Legal and governance frameworks	Development in accordance to the observance of the rule of law, sound economic governance and appropriate transparency.
3. Data privacy	Rigorous standards of privacy, accountability for the protection of users' data, and transparency.
4. Operational resilience and cybersecurity	CBDC ecosystem must be secure and resilient to cyber, fraud and other operational risks.
5. Competition	Coexistence with existing means of payment and CBDC operating in an open, secure, resilient, transparent and competitive environment.

6. Illicit finance	Faster, more accessible, safer and cheaper payments with a commitment to mitigate their use in facilitating crime.
7. Spillovers	Avoiding risks of harm to the international monetary and financial system.
8. Energy and Environment	Efficient energy usage of any CBDC infrastructure to support the international community's shared commitments to transition to a 'net zero' economy.
Opportunities	
9. Digital economy and innovation	Be a catalyst for responsible innovation in the digital economy and ensure interoperability with existing and future payments solutions.
10. Financial inclusion	Not impeding and where possible enhancing access to payment services for those excluded from or underserved by the existing financial system, while also complementing the important role that will continue to be played by cash.
11. Payments to and from the public sector	Supporting payments between authorities and the public in a fast, inexpensive, transparent, inclusive and safe manner, both in normal times and in times of crisis.
12. Cross-border functionality	Enhancing cross-border payments, including through central banks, and other organisations and considering the international dimensions of CBDC design.
13. International development	Safeguard key public policies of the issuing and recipient countries, while providing sufficient transparency about the nature of the CBDC's design features.

Table 6: Public Policy Principles for Retail Central Bank Digital Currencies (G7, 2021)

Inclusion, Privacy, Resilience, Cybersecurity and Interoperability are some of the key aspects that both sets of Principles share. Since not only CBDC is set to depend on

efficient identification, but also both share principles upon which they need to be built upon, simultaneously developing CBDC and digital ID can help to achieve efficient solutions and avoid fragmentation.

3.3. Key insights

While both CBDC and digital ID are still in their early stages of development, the impact that both can have in our increasingly digital worlds is immense. While the design of both remains unclear, we can already identify some of the trends that can potentially shape how they will develop in the future. Given that there are few practical applications of discussed concepts, there is a lack of empirical studies but from existing research and case studies, it can be established that:

- Secure and efficient identification is vital for the rollout of retail account-based CBDC, thus, digital identity has a major role to play in this context.
- While CBDC is set to complement and potentially in the long run replace cash, it must be established how it can leverage secure identification and anonymity. As anonymity is a feature of cash, people might be reluctant to adopt CBDC if it cannot ensure payers' integrity. Pseudonymity might hold an answer to this dilemma.
- A two-tier system seems like the best solution for CBDC. In this scenario, central banks will most likely ensure the stability of the system while private sector players will interact with users and take responsibility for many operational tasks, including identification. Current KYC checks still rely on manual processes and lack efficiency and security. Thus, the private sector can play a significant role as an innovator in establishing next-generation digital ID solutions.
- Decentralised identity can be the future of digital ID and play an instrumental role in ensuring privacy and security in CBDC. Its benefits extend way beyond CBDC but it is not covered in this paper.
- Digital identity as well as CBDC need to cater for different cultures and societal needs, while also ensuring interoperability across borders and platforms.
- One identity or one currency that caters to all sounds like a utopia and is unlikely to work. Instead establishing unifying standards and guidelines on technical interoperability is crucial. The EU is already working on creating a common toolbox towards a European Digital Identity Framework.

- It is important to establish a clear definition of what a digital identity is and what it includes, as there are many interpretations of it and it might hinder the creation of a common framework.
- Harnessing data in digital identities can bring new opportunities to provide users with a personalised experience and better risk management, but it must be ensured that in this case one's freedom of choice is maintained and human rights are not infringed.
- Policymakers need to carefully analyse what business models might emerge in the development of digital identity and CBDC, what can be incentives for private parties to participate in this development, and promote competition by advocating entry of new players and innovative solutions.

3.4. Recommendations for future research

As it was mentioned before, CBDC and digital ID are still in their infancy, and consequently, there is plenty of room for research to be carried out on these topics. There is a very clear gap in the research on digital identity, as in general there is very little research done on this topic and there have only been some recent strides from the decentralised identity perspective. More research needs to be carried out on digital identity to evaluate how it can function in society, evaluating optimal design choices in detail with attention to what roles private and public sectors would play. Identification in terms of account-based CBDC is another critical topic that requires to dwell deep into. Most of the work currently just barely touches upon the identification and KYC of account-based CBDC, and we need to establish how both can work together for successful implementation in practice. As there is a lack of empirical research, analysing case studies in detail can help to identify lessons learned and set precedents. Cases of Singapore, Sweden, Norway, and South Korea can be assessed to identify what we can learn for future development. Meanwhile, cases of Mexico, Taiwan, Kenya, and Argentina can help us to understand what needs to be avoided in the development of a successful and secure digital ID. Experience with the implementation of FPS can help to establish lessons learned from bringing innovation in the payments system, and potentially can support the building of the CBDC system. Examples of Sweden, South Korea and Brazil can serve as guidance for lessons learned.

Conclusions

The goal of this study was to evaluate the connection between digital identity and central bank digital currencies, and consequently assess the current stage of both. Since both digital identity and CBDCs are in their early stages of development, there is a lack of research available on both with many unknowns remaining. While CBDC has gained significant attention over the past years, digital identity progress has been slow. It has become apparent that there is a lack of empirical studies and many concepts still remain theoretical. Regarding CBDC, the majority of countries are putting strides into researching and developing their CBDCs but there has been a lack of analysis on design choices and reasoning behind them. While there may not be a one-fits-all solution, one of the main benefits of CBDC is cross-border and potentially cross-platform interoperability. To ensure that, countries need to establish shared guidelines to follow, as fragmented design choices can put significant limitations on interoperability. The goal of this paper was to summarise the current CBDC design trajectory based on the existing research, case studies and an interview with Gabriela Guibourg, Head of Analysis and Policy at the Payments Department at Riksbank. It is suggested that retail CBDC can have the most impact, while it also must be tied to digital identity as an account-based CBDC and established on a two-tier system that relies on public-private sector cooperation. Digital identity is critical for an account-based CBDC, but digitizing KYC, AML, CTF, and CDD compliance has been slow progress and the first attempts at the next-generation digital identity design are only emerging now. Decentralised identity, even though a complex design, holds a lot of potential to allow better flexibility for users, and enhance security and privacy. Pseudonymous digital identity design can allow users to disclose only the information needed while also allowing to ensure traceability and regulatory compliance in the system. CBDC depends on an efficient solution for digital identification. Both share not only technological challenges but also principles to follow, namely, privacy, resilience, security, inclusion and interoperability. In the future, the only thing we may need to transact may be our identity, and that can be the case with an account-based CBDC. But to achieve that it is vital for digital identity and CBDC to develop simultaneously with both public and private parties involved.

References

Libra Association, 2019. *An Introduction to Libra.* s.l., Libra Association.

Access Now, 2021. *The Mexican unique digital ID (CUID) proposal threatens human rights.* [Online]
Available at:
https://www.accessnow.org/cms/assets/uploads/2021/09/The_Mexican_unique_digital_ID_CUID_proposal_threatens_human_rights.pdf
[Accessed 19 November 2022].

Adrian, T. & Mancini-Griffoli, T., 2019. The Rise of Digital Money. *Annual Review of Financial Economics*, 3 May, p. 13:57–77.

Armelius, H., Claussen, C. A. & Hull, I., 2021. *On the possibility of a cash-like CBDC,* s.l.: Sveriges Riksbank Staff memo.

Arner, D. W., Barberis, J. & Buckley, R. P., 2016. FinTech, RegTech and the Reconceptualization of Financial Regulation. *Northwestern Journal of International Law and Business,* October.

Arner, D. W., Zetzsche, D. A., Buckley, R. P. & Barberis, J. N., 2018. The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities. *University of New South Wales Law Research Series*.

Atlantic Council, 2022. *Central Bank Digital Currency Tracker.* [Online]
Available at: https://www.atlanticcouncil.org/cbdctracker/
[Accessed 3 November 2022].

Auer, R. & Böhme, R., 2020. The technology of retail central bank digital currency. *BIS Quarterly Review*, March.

Börü, A., 2022. *Central Bank of Turkey Plans to Launch a CBDC in 2023.* [Online]
Available at: https://www.coindesk.com/policy/2022/10/25/central-bank-of-turkey-plans-to-launch-a-cbdc-in-2023/
[Accessed 19 November 2022].

Bae, J., 2022. The Bank of Korea's CBDC research: current status and key considerations. *BIS Papers No 123 CBDCs in emerging market economies,* April, pp. 107-116.

Birch, D., 2014. *Identity is the New Money.* 1st Edition ed. London: London Publishing Partnership.

BIS, 2021. *Annual Economic Report,* s.l.: Bank for International Settlements.

Bordo, M. D. & Levin, A. T., 2017. CENTRAL BANK DIGITAL CURRENCY AND THE FUTURE OF MONETARY POLICY. *NBER WORKING PAPER SERIES. NATIONAL BUREAU OF ECONOMIC RESEARCH,* August.Volume Working Paper 23711.

Brainard, L., 2021. *Private Money and Central Bank Money as Payments Go Digital: an Update on CBDCs.* Washington, D.C., Consensus by CoinDesk 2021 Conference.

Brunnermeier, M. K., James, H. & Landau, J.-P., 2019. *The Digitalization of Money,* s.l.: s.n.

Brunnermeier, M. K. & Niepelt, D., 2019. *On the Equivalence of Private and Public Money,* s.l.: NATIONAL BUREAU OF ECONOMIC RESEARCH Working Paper 25877.

Burt, C., 2021. *Kenya's digital ID ruled illegal until data protection impact assessment completed.* [Online]
Available at: https://www.biometricupdate.com/202110/kenyas-digital-id-ruled-illegal-until-data-protection-impact-assessment-completed
[Accessed 19 November 2022].

Camenisch, J. & Lysyanskaya, A., 2001. An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2001: Advances in Cryptology),* pp. 93-118.

Cameron, K., 2005. *The Laws of Identity.* [Online]
Available at: https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf
[Accessed 11 November 2022].

Catalini, C., Dai Li, W., de Gortari, A. & Lilley, A., 2021. *From Stablecoins to CBDCs: The Public Benefits of a Public-Private Partnership,* s.l.: s.n.

Catalini, C. & de Gortari, A., 2021. *On the Economic Design of Stablecoins,* s.l.: s.n.

Catalini, C. & Massari, J., 2021. *Stablecoins and the Future of Money.* [Online]
Available at: https://hbr.org/2021/08/stablecoins-and-the-future-of-money
[Accessed 2 November 2022].

Cimpanu, C., 2021. *Hacker steals government ID database for Argentina's entire population.* [Online]
Available at: https://therecord.media/hacker-steals-government-id-database-for-argentinas-entire-population/
[Accessed 19 November 2022].

CoinMarketCap, 2022. *Tether.* [Online]
Available at: https://coinmarketcap.com/currencies/tether/
[Accessed 22 November 2022].

d'Avernas, A., Maurin, V. & Vandeweyer, Q., 2022. *Can Stablecoins be Stable?,* s.l.: s.n.

Duffie, D., 2019. *Digital Currencies and Fast Payment Systems: Disruption is Coming.* s.l., For presentation to the Asian Monetary Policy Forum.

Duffie, D., 2021. Testimony of Darrell Duffie. *Hearing on "Building a Stronger Financial System: Opportunities of a Central Bank Digital Currency"*, 9 June.

Duffie, D., Mathieson, K. & Pilav, D., 2021. *Central Bank Digital Currency Principles for Technical Implementation,* s.l.: s.n.

Eichengreen, B., 2019. *FROM COMMODITY TO FIAT AND NOW TO CRYPTO: WHAT DOES HISTORY TELL US? ,* s.l.: NATIONAL BUREAU OF ECONOMIC RESEARCH Working Paper 25426.

European Central Bank, 2019. Exploring anonimity in central bank digital currencies. *In Focus,* Issue Issue no 4.

European Central Bank, 2021. *Eurosystem report on the public consultation on a digital euro,* s.l.: Eurosystem report on the public consultation on a digital euro.

European Commission, 2021a. *COMMISSION RECOMMENDATION of 3.6.2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework,* Brussels: European Commission.

European Commission, 2021b. *Commission proposes a trusted and secure Digital Identity for all Europeans.* [Online]
Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663
[Accessed 15 November 2022].

European Union, 2016. REGULATION (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 Reg. *Official Journal of the European Union,* Volume Article 17.

Fitri, A., 2022. *The state of digital identity in Europe.* [Online]
Available at: https://techmonitor.ai/digital-identity/the-state-of-digital-identity-in-europe
[Accessed 15 November 2022].

G7, 2021. *Public Policy Principles for Retail Central Bank Digital Currencies (CBDCs),* London: G7.

Goodell, G. & Aste, T., 2019. A Decentralized Digital Identity Architecture. *Frontiers in Blockchain,* 2(17).

Gross, J., 2019. *Libra: insights into its expected stability.* [Online]
Available at: https://jonasgross.medium.com/libra-insights-into-its-expected-stability-a4d5cfbfec1b
[Accessed 6 November 2022].

Guibourg, G., 2022. *The interview on CBDC* [Interview] (22 November 2022).

Hersey, F., 2022. *Singpass incorporates digital identity card, saves $36 per onboarding, considers decentralization.* [Online]
Available at: https://www.biometricupdate.com/202207/singpass-incorporates-digital-identity-card-saves-36-per-onboarding-considers-decentralization
[Accessed 19 November 2022].

Kereiakes, E., Kwon, D., Di Maggio, M. & Platias, N., 2019. *Terra Money: Stability and Adoption,* s.l.: s.n.

Kim, S., 2022. *South Korea Aims to Boost Economy With Digital ID on Blockchain.* [Online]
Available at: https://www.bloomberg.com/news/articles/2022-10-16/south-korea-aims-to-boost-economy-with-digital-id-on-blockchain
[Accessed 19 November 2022].

Kinberg Batra, A., 2022. *DN Debatt. ”Sverige måste införa en statlig e-legitimation”.* [Online]
Available at: https://www.dn.se/debatt/sverige-maste-infora-en-statlig-e-legitimation/
[Accessed 21 November 2022].

Klosters, D., 2018. Digital Identity. On the Threshold of a Digital Identity Revolution. *World Economic Forum White Paper*, January.

Kosse, A. & Mattei, I., 2022. *Gaining momentum – Results of the 2021 BIS survey on central bank digital currencies.* [Online]
Available at: https://www.bis.org/publ/bppdf/bispap125.pdf

Masiero, S. & Bailur, S., 2021. Digital identity for development: The quest for justice and a research agenda. *Information Technology for Development,* 27(1), pp. 1-12.

Morales-Resendiz, R. et al., 2021. Implementing a retail CBDC: Lessons learned and key insights. *Latin American Journal of Central Banking,* 2(1), p. 100022.

Nakamoto, S., 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System,* s.l.: s.n.

Nyst, C., Pannifer, S., Whitley, E. & Makin, P., 2016. *Digital Identity: Issue Analysis,* s.l.: Consult Hyperion.

Organization for Security and Co-operation in Europe, 2003. *Council of Europe: Declaration on freedom of communication on the Internet.* [Online]
Available at: https://www.osce.org/fom/31507
[Accessed 21 November 2022].

Ozili, P. K., 2022. Central bank digital currency research around the world: a review of literature. *Journal of Money Laundering Control,* Volume 1368-5201.

Portulans Institute, 2022. *Network Readiness Index.* [Online]
Available at: https://networkreadinessindex.org/country/korea-rep/
[Accessed 19 November 2022].

Reuters, 2017. *Brazil Congress passes law restricting online criticism of candidates.* [Online]
Available at: https://www.reuters.com/article/brazil-politics-censorship-idUSL8N1MG6GV
[Accessed 22 November 2022].

Reuters, 2019. *China's digital currency not seeking 'full control' of individuals' details - central bank official.* [Online]

Available at: https://www.reuters.com/article/china-markets-digital-currency-idINKBN1XM0JA
[Accessed 5 November 2022].

Sandor, K. & Genç, E., 2022. *The Fall of Terra: A Timeline of the Meteoric Rise and Crash of UST and LUNA.* [Online]
Available at: https://www.coindesk.com/learn/the-fall-of-terra-a-timeline-of-the-meteoric-rise-and-crash-of-ust-and-luna/
[Accessed 16 November 2022].

Soderberg, G., 2022. Behind the Scenes of Central Bank Digital Currency Emerging Trends, Insights, and Policy Lessons. *International Monetary Fund FINTECH NOTE*, February, p. Note 2022/004.

Spencer, . E. A. & Mahtani, K., 2017. *Hawthorne effect.* [Online]
Available at: https://catalogofbias.org/biases/hawthorne-effect/
[Accessed 15 November 2022].

Statista, 2022. *Estimate of the market capitalization of algorithmic stablecoin from December 2020 to June 21, 2022.* [Online]
Available at: https://www-statista-com.ez.hhs.se/statistics/1316227/algorithmic-stablecoin-market-value/
[Accessed 5 November 2022].

Statista, 2022. *Market capitalization of the 10 biggest stablecoins from January 2017 to June 19, 2022.* [Online]
Available at: https://www-statista-com.ez.hhs.se/statistics/1255835/stablecoin-market-capitalization/
[Accessed 5 November 2022].

Statista, 2022. *Number of users of Alipay and WeChat Pay in China in 2020, with forecasts from 2021 to 2025.* [Online]
Available at: https://www-statista-com.ez.hhs.se/statistics/1271130/mobile-wallet-user-forecast-in-china/
[Accessed 21 November 2022].

Sveriges Riksbank, 2022. *E-krona pilot Phase 2,* s.l.: s.n.

Sveriges Riksbank, 2022. *Payments Inquiry – the state's role in the payment market.* [Online]
Available at: https://www.riksbank.se/en-gb/payments--cash/the-riksbanks-task-in-relation-to-payments/payments-inquiry--the-states-role-in-the-payment-market/
[Accessed 22 November 2022].

Swiss Federal Department of Justice and Police, 2021. *Elektronische Identität: das E-ID-Gesetz.* [Online]
Available at:
https://www.ejpd.admin.ch/ejpd/de/home/themen/abstimmungen/bgeid.html
[Accessed 5 November 2022].

Tether, 2014. *Tether: Fiat currencies on the Bitcoin blockchain.* [Online]
Available at: https://tether.to/en/whitepaper/
[Accessed 6 November 2022].

The Cambridge Centre for Alternative Finance, 2021. *Cambridge Bitcoin Electricity Consumption Index.* [Online]
Available at: https://ccaf.io/cbeci/index/comparisons
[Accessed 4 November 2022].

Verborgh, R., 2019. *Re-decentralizing the Web, for good this time.* [Online]
Available at: https://ruben.verborgh.org/articles/redecentralizing-the-web/
[Accessed 14 November 2022].

Wagner, K. et al., 2018. *Self-sovereign identity. A position paper on blockchain enabled identity and the road ahead,* Berlin: German Blockchain Association.

Wemnell, M., 2019. *Statistik BankID – användning och innehav - fördjupning.* [Online]
Available at: https://www.bankid.com/assets/bankid/stats/2019/statistik-2019-01.pdf
[Accessed 19 November 2022].

Wind, P., 2019. *What Is a Stablecoin?.* [Online]
Available at: https://coincodex.com/article/2932/what-is-a-stablecoin/
[Accessed 3 November 2022].

World Bank Group, 2018. *G20 Digital Identity Onboarding,* Washington DC: The World Bank Group.

World Bank Group, 2021. *Central Bank Digital Currency. A Payments Perspective,* Washington DC : The World Bank.

World Economic Forum, 2018. *Identity in a Digital World: A new chapter in the social contract,* Cologny/Geneva: World Economic Forum.

World Economic Forum, 2020. Reimagining Digital Identity: A Strategic Imperative. *Community Paper*, January.

Yang, S., 2021. *Taiwan's digital ID plan halted.* [Online]
Available at: https://www.taiwannews.com.tw/en/news/4100464
[Accessed 22 November 2022].

Zetzsche, D. A., Arner, D. W., Buckley, R. P. & Weber, R. H., 2019. The Future of Data-Driven Finance and RegTech: Lessons from EU Big Bang II. *University of Luxembourg Law Working Paper Series* , 1 March, pp. Paper number 2019-005.

Zwitter, A. J., Gstrein, O. J. & Yap, E., 2020. Digital Identity and the Blockchain: Universal Identity Management and the Concept of the "Self-Sovereign" Individual. *Frontiers in Blockchain,* 3(26).

Appendix

	CBDC				Digital ID
Country	**CBDC stage**	**Use case**	**Underlying technology**	**Access**	**Digital ID stage**
The Bahamas	Launched	Retail	Both	Both	Development
Nigeria	Launched	Retail	DLT	Account	Development
Jamaica	Launched	Retail	Conventional	Account	Pilot
Anguilla	Launched	Retail	DLT	Both	Research
Saint Kitts and Nevis	Launched	Retail	DLT	Both	Research
Antigua and Barbuda	Launched	Retail	DLT	Both	Research
Montserrat	Launched	Retail	DLT	Both	Research
Dominica	Launched	Retail	DLT	Both	Research
Saint Lucia	Launched	Retail	DLT	Both	Research
Saint Vincent and the Grenadines	Launched	Retail	DLT	Both	Research
Grenada	Launched	Retail	DLT	Both	Research
Sweden	Pilot	Retail	DLT	Both	Mature
Russia	Pilot	Retail	Both	Account	Development
Kazakhstan	Pilot	Retail	Both	Token	Pilot
China	Pilot	Both	Both	Account	Pilot
Thailand	Pilot	Both	Both	Both	Active
United Arab Emirates	Pilot	Wholesale	DLT	Account	Active
Saudi Arabia	Pilot	Wholesale	DLT	Account	Active
South Africa	Pilot	Both	Undecided	Token	Development

South Korea	Pilot	Retail	DLT	Undecided	Pilot
Lithuania	Pilot	Retail	Undecided	Undecided	Active
Hong Kong	Pilot	Both	Undecided	Undecided	Active
Singapore	Pilot	Wholesale	Undecided	Undecided	Mature
Malaysia	Pilot	Wholesale	Undecided	Undecided	Pilot
Ghana	Pilot	Retail	Undecided	Undecided	Partly active
Ukraine	Pilot	Undecided	Undecided	Undecided	Active
Canada	Development	Both	Both	Both	Development
Brazil	Development	Retail	DLT	Token	Pilot
Netherlands	Development	Retail	Both	Account	Active
India	Development	Both	Both	Account	Active
Cambodia	Development	Retail	DLT	Token	Pilot
Estonia	Development	Retail	DLT	Undecided	Mature
Germany	Development	Undecided	Both	Both	Active
Spain	Development	Retail	Undecided	Both	Partly active
Italy	Development	Undecided	Both	Both	Active
Turkey	Development	Retail	Undecided	Undecided	Active
Palau	Development	Both	DLT	Undecided	Active
Bahrain	Development	Wholesale	Both	Undecided	Partly active
Israel	Development	Retail	Both	Undecided	Development
Haiti	Development	Both	Both	Undecided	Stagnant
Japan	Development	Both	Undecided	Undecided	Pilot
Venezuela	Development	Both	Undecided	Undecided	Partly active
Switzerland	Development	Wholesale	Undecided	Undecided	Active
France	Development	Both	Undecided	Undecided	Active
Lebanon	Development	Retail	Undecided	Undecided	Research
Iran	Development	Retail	Undecided	Undecided	Pilot
Bhutan	Development	Both	Undecided	Undecided	Partly active
Indonesia	Development	Both	Undecided	Undecided	Development
Australia	Development	Both	Undecided	Undecided	Active
Mauritius	Development	Both	Undecided	Undecided	Active
Belize	Development	Undecided	Undecided	Undecided	Partly active

Iceland	Research	Retail	Undecided	Both	Active
Austria	Research	Wholesale	DLT	Undecided	Partly active
Morocco	Research	Retail	Undecided	Token	Active
Palestine	Research	Retail	Undecided	Undecided	Development
Tunisia	Research	Wholesale	Undecided	Undecided	Research
Georgia	Research	Retail	Undecided	Undecided	Stagnant
UK	Research	Both	Undecided	Undecided	Development
Norway	Research	Retail	Undecided	Undecided	Mature
US	Research	Both	Undecided	Undecided	Research
Mexico	Research	Retail	Undecided	Undecided	Development
Chile	Research	Retail	Undecided	Undecided	Development
Hungary	Research	Retail	Undecided	Undecided	Partly active
Kuwait	Research	Retail	Undecided	Undecided	Active
Pakistan	Research	Retail	Undecided	Undecided	Partly active
Kenya	Research	Retail	Undecided	Undecided	Halted
Madagascar	Research	Retail	Undecided	Undecided	Pilot
Eswatini	Research	Both	Undecided	Undecided	Partly active
Laos	Research	Both	Undecided	Undecided	Research
Taiwan	Research	Both	Undecided	Undecided	Halted
Philippines	Research	Retail	Undecided	Undecided	Development
New Zealand	Research	Retail	Undecided	Undecided	Development
Vietnam	Research	Undecided	Undecided	Undecided	Partly active
Myanmar	Research	Undecided	Undecided	Undecided	Development
Bangladesh	Research	Undecided	Undecided	Undecided	Development
Nepal	Research	Undecided	Undecided	Undecided	Development
Czech Republic	Research	Undecided	Undecided	Undecided	Active
Guatemala	Research	Undecided	Undecided	Undecided	Stagnant
Honduras	Research	Undecided	Undecided	Undecided	Partly active
Trinidad and Tobago	Research	Undecided	Undecided	Undecided	Research
Colombia	Research	Undecided	Undecided	Undecided	Partly active

Peru	Research	Undecided	Undecided	Undecided	Partly active
Paraguay	Research	Undecided	Undecided	Undecided	Active
Belarus	Research	Undecided	Undecided	Undecided	Active
Jordan	Research	Undecided	Undecided	Undecided	Active
Qatar	Research	Undecided	Undecided	Undecided	Active
Oman	Research	Undecided	Undecided	Undecided	Stagnant
Uganda	Research	Undecided	Undecided	Undecided	Development
Rwanda	Research	Undecided	Undecided	Undecided	Development
Tanzania	Research	Undecided	Undecided	Undecided	Development
Zambia	Research	Undecided	Undecided	Undecided	Development
Zimbabwe	Research	Undecided	Undecided	Undecided	Development
Namibia	Research	Undecided	Undecided	Undecided	Development
Macau	Research	Undecided	Undecided	Undecided	Development
Tonga	Research	Undecided	Undecided	Undecided	Development
Fiji	Research	Undecided	Undecided	Undecided	Research
Vanuatu	Research	Undecided	Undecided	Undecided	Pilot
Sint Maarten	Inactive	Retail	Conventional	Token	Research
Curaçao	Inactive	Retail	Conventional	Token	Stagnant
Uruguay	Inactive	Retail	Conventional	Token	Development
Denmark	Inactive	Retail	Undecided	Both	Mature
Finland	Inactive	Retail	Both	Undecided	Active
Argentina	Inactive	Undecided	Undecided	Undecided	Active
Bermuda	Inactive	Undecided	Undecided	Undecided	Development
Egypt	Inactive	Undecided	Undecided	Undecided	Development
Azerbaijan	Inactive	Undecided	Undecided	Undecided	Development
North Korea	Inactive	Undecided	Undecided	Undecided	Stagnant
Ecuador	Cancelled	Retail	Conventional	Account	Development
Senegal	Cancelled	Retail	Undecided	Token	Pilot