"The Other Side of the Coin: Exploring the Privacy Implications of the Digital Euro"

Olij, V.J. (s1697277)
20-8-2024
Els de Busser
Crisis and Security Management
Word count: 18223

Abstract

This thesis examines the cyber privacy risks of the European Central Bank's digital euro, focusing on both its online and offline forms. Because of emerging private digital currencies, central banks are prompted to develop their own alternatives, such as the digital euro. This study investigates whether the digital euro offers greater privacy than commercial bank money, considering the new infrastructure and technologies involved. Through a theoretical framework on privacy, cybersecurity, and the nature of CBDCs, the research compares the digital euro to cash and commercial bank money. The findings suggest that while the online digital euro may provide more privacy than commercial bank money, the offline version is not as private as cash. Furthermore, the ECB lack focus on the socio-technical aspects of cyber privacy risks.

Contents

LIST OF ACRONYMS

AML/CFT	Anti-Money Laundering and Countering the Financing of Terrorism
ATM	Automated Teller Machine
CBDC	Central Bank Digital Currency
CIA	Confidentiality, Integrity and Availability
DEAN	Digital Euro Account Number
DDoS	Distributed Denial of Service
DLT	Distributed Ledger Technology
ECB	European Central Bank
EU	European Union
GDPR	General Data Protection Regulation
ICT	Information and Communication Technology
IMF	International Monetary Fund
KYC	Know Your Customer
NFC	Near-Field Communication
P2P	Peer-to-peer
POS	Point Of Sale
PSP	Payment Service Provider
SAP	Single Access Point
UTXO	Unspent Transaction Output

1. Introduction

In recent years, the discourse surrounding central bank digital currencies (CBDCs) has gained significant momentum. This reflects the broader digital transformation of the global financial landscape. Since the emergence of Bitcoin in 2009 , numerous private, decentralized digital currencies have emerged, prompting central banks to explore their own alternatives. As of May 2024, 134 countries, representing 98% of global GDP, are actively exploring CBDCs (Atlantic Council, n.d.). Among these institutions is the European Central Bank (ECB), which is in the process of developing its own CBDC, the digital euro. This new currency could offer certain benefits such as enhanced financial inclusion, as highlighted by Queen Máxima of the Netherlands (2022). Also, it could enhance payment efficiency and central banks could cement their place in the digitized financial landscape (Ward & Rochemont, 2019, p. 9).

However, among these opportunities are challenges with introducing the digital euro. As often with new developments, there are concerns about the end users' data protection of the CBDC, in terms of privacy and cybersecurity. On the one hand, in this new context the ECB could potentially gain access to greater amounts of personal financial data that could pose risks to user privacy. The importance of the privacy protection of the digital euro has been underscored in various EU documents, including the Eurosystem Report on a digital euro (ECB, 2020a), the ECB's public consultation (ECB, 2020b), and the European Commission's targeted consultation (European Commission, 2022). The ECB addresses these challenges by aiming to develop a digital euro that will be more private and more secure than commercial bank money, even planning to issue an offline variant (ECB, 2024e). On other hand, CBDCs are likely to depend on more modern technologies, which risks are lesser known and could create blind spots in the cybersecurity, especially with two variants of the digital euro. The European Commission requested a Joint Opinion by the European Data Protection Supervisor (EDPS) and the European Data Protection Board (EDPB) to evaluate the digital euro proposal (European Commission, 2023b). This publication focuses mainly on the lawful processing of personal data and marginally on unlawful data processing, like malicious data breaches.

This thesis addresses these concerns by investigating the personal privacy risks and cybersecurity challenges associated with the potential implementation of both the online and offline digital euro. The EU plays a major role in the protection of personal data, as exemplified by the General Data Protection Regulation (GDPR), which also dictates the

framework for the digital euro implementation. Understanding these issues is not only crucial for a successful adoption of the digital euro, but also for maintaining public trust in the financial system. With alternatives in the form of cash and commercial bank money, people are not inclined to use a currency they don't trust. Therefore, the adoption of the digital euro entirely depends on the currency providing more benefits than alternatives, like offering greater privacy. In an increasingly interconnected world, where e-commerce is becoming the norm, data protection is more important than ever (Bhatia et al., 2021). This research is therefore aimed at policymakers, regulators and the broader public alike.

From an academic perspective, this thesis contributes to an underexplored area of research. While much of the current literature on CBDCs is anchored in economics or finance, the privacy and cybersecurity dimensions have often been overshadowed. A literature review by Tronnier et al. (2020) highlights a gap in the legal and societal aspects of CBDCs. By offering a comprehensive, interdisciplinary analysis that integrates themes of digital currencies, privacy, cybersecurity, and risk management, this study aims to fill a critical gap in the academic discourse. Moreover, as the digital euro is still in the development phase, this research provides a timely foundation for understanding its potential implications, offering insights that are crucial for both scholarly inquiry and practical policy formulation.

1.1. Research Question

In order to come up with a valid assessment of the cyber privacy risks of the digital euro, this research places the digital euro in context of the current financial landscape. A comparison with cash and commercial bank money provide meaning to the design choices of the digital euro. Hence, the research question of this thesis is: *"How do the cyber privacy risks for end users of the digital euro in both its online and offline implementations compare to existing forms of money, such as cash and commercial bank money?"*

1.2. Reading Guide

The structure of this research is as follows: After this introductory chapter, the thesis has two chapters dedicated to building a theoretical framework. Chapter two focuses on academic research related to the rights of privacy and data protection and the concepts of cybersecurity and risk, providing the conceptual half of the theoretical framework to analyze the digital euro. Chapter three then dissects the concept of CBDC, exploring its emergence, role in the

financial landscape, and various designs. The design choices made by central banks differ heavily, due to different goals, and have different implications on privacy and cybersecurity. Together, these two chapters offer a lens through which the cyber privacy risks of the digital euro can be examined. The fourth chapter outlines the methodology used in the research with some insight in how the stages of research are conducted. Then, the fifth chapter applies the theoretical framework to the case of the digital euro. There will be a combination of the design choices of the digital euro in both its forms and an assessment of the cyber privacy risks. The next chapter is the discussion, where the implications of these findings are compared to the current financial landscape. The thesis concludes with a conclusion and end with a bibliography.

2. Theoretical foundations

At the base of EU's privacy regulations is the GDPR, which adopts a risk-based approach and consider the cybersecurity part of the data processor's responsibility. Hence, this first half of the theoretical framework covers privacy, cybersecurity and risk. In order to answer the research question, it is necessary to clarify the relevant concepts and to establish a framework that can be applied to the case.

2.1. Privacy and Data Protection

Digital innovations often deals with an increasing amount of personal data and consequently needs to balance this with privacy protection (Harvey, 2013; Zarsky, 2015; Aiello, 2024). CBDCs are no exception, although the degree in which privacy issues are involved depends significantly on the design choices and implementation of the currency. Given that all CBDC variations, including the digital euro, involve personal data to some extent, this section will discuss privacy and data protection rights in the context of CBDCs. CBDCs could either compromise user privacy or potentially enhance user privacy compared to traditional payment methods.

2.1.1. The Right to Privacy

Defining privacy is challenging, as the concept is highly context-dependent (Banisar & Davies, 1999, p. 6). Article 12 of the Universal Declaration of Human Rights (UDHR) states: "No one shall be subjected to arbitrary interference with his privacy, family, home or

correspondence, nor to attacks upon his honor and reputation" (UDHR, 1948, Article 12). However, this article mentions the terms privacy, but does not describe what is meant by it. Warren and Brandeis (1890, p. 193) established the concept of privacy as the "right to be let alone," recognizing one's right to spiritual nature, feelings, and intellect.
The right to privacy has gained an increasing relevance since the development of the Internet (Chung & Paynter, 2002; Collier, 1995). The advent of modern information and communications technology (ICT) added a new dimension to the concept of privacy. In the 1960s, discussions began about privacy-related threats posed by ICT, particularly in the United States (Bygrave, 2010, p. 167). Despite its influence, these discussions often avoided explicitly using the term "privacy," preferring "data protection," derived from the German term "Datenschutz" (Bygrave, 2010, p. 168).

2.1.2. Privacy vs. Data Protection

While privacy and data protection are related, they are not the same. Privacy is one of the most challenging rights to define, whereas data protection is more straightforward for legal scholars (Tzanou, 2013, p. 88). Data protection has more practical implications than privacy, focusing on concrete principles such as: "collection and purpose limitation, data quality, data security, openness and transparency of processing, accountability, individual participation principle (Tzanou, 2013, p. 88)." Moreover, data protection is about informational autonomy, not just informational privacy (Tzanou, 2023, p. 88). It involves actively deciding what happens to one's data, not merely safeguarding it against intrusion. De Hert and Gutwirth (2009) describe data protection as "a catch-all term for a series of ideas regarding the processing of personal data." Both processing and personal data require clarification.

Personal data

What personal data entails, depends on jurisdiction and culture. In case of the digital euro, the relevant jurisdiction is the EU and the applicable law is the GDPR, which defines personal data as:

"any information which are related to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological,

genetic, mental, economic, cultural or social identity of that natural person" (GDPR, 2016, art. 4).

This definition is broad. Not only are the ways of identifying someone extensive, the identification is considered both directly and indirectly. Indirect identification could refer to identification through the unique combination of non-unique identifiers, distinguishing a person (Purtova, 2022, p. 175).

Processing of personal data

In the same article 4, processing is defined as:

"any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction" (GDPR, 2016).

Again, this definition is quite comprehensive. The act of processing refers to numerous methods, but crucial is that this definition encompasses both manual and automated processing. These conceptualizations of "personal data" and "processing" provide a depth and thoroughness to the protection of people's data and imposes a great responsibility on data processors. Every single use of a personal data must have a documented legal basis (Arfelt, Basin & Debois, 2019, p. 681).

Article 5 (GDPR, 2016) relates to the processing of personal data and states on the one hand that data should be processed "lawfully, fairly and in a transparent manner" and on the other hand "adequate, relevant and limited", which is also known as data minimization. This article's scope is the authorized access to personal data and is about ensuring the confidentiality, integrity and availability of data, also known as the CIA triad. Article 32 (GDPR, 2016), on the other hand concerns the unauthorized access to personal data. Article 32 is about the security of processing, conducting a risk-based approach. This risk-based approach takes into account the "state of the art", which implies that security measures should be based on proven knowledge and at an advanced state of technical development (Selzer, 2021, p. 122). This is done through technical and organizational measures, such as

pseudonymization and encryption of personal data (GDPR, article 32, 2016). The GDPR (article 4, 2016) describes pseudonymization as the processing of personal data where additional information is needed to attribute the data to a specific data subject. A digital pseudonym uses a bit of string as an identifier to the personal data instead of the personal data itself (Pfitzmann & Hansen, 2010, p. 24). This additional piece of information serves as a key to decrypt that bit of string, so that only those with the key can access the data (Garg et al., 2013, p. 467). The key is stored separately, but anyone with this key has access the encrypted data. Although not directly identifiable, this means that pseudonymized data is still personal data and therefore falls under GDPR, in contrast to anonymized data. According to Recital 26 (GDPR, 2016), anonymous data is personal data, which is rendered in such a manner that the subject is no longer identifiable. The difference between pseudonymized and anonymized data is the fact that pseudonymized data can be decrypted and disclose the potentially personal data, where anonymized data never contained personal data in the first place or not anymore (Finck & Pallas, 2020, p. 14). In other words, pseudonymized data is temporarily disconnected from personal data, while anonymized data is permanently disconnected from the personal data. These methods and techniques can be combined; anonymous data can also be pseudonymized. This significantly reduces the risk of exposing personal data. The GDPR's emphasis on cybersecurity measures led to widespread European implementation of "state-of-the-art technologies, encryption protocols and employee training programs" (Amoo et al., 2024, p. 1341).

Article 5 and 32 discusses how personal data should be processed in order to prevent data breaches. Article 33 (GDPR, 2016) states that in case of a data breach, the supervisory authority should be notified within 72 hours. Organizations may try to omit this obligation, but this article prevents the notion that one is innocent until proven guilty, since this reporting obligation stops organizations to try to be absolved of their responsibilities (Shastri, Wasserman & Chidambaram, 2019, p. 5). Furthermore, article 25 (GDPR, 2016) states that privacy should be embedded by design and by default, which applies to the development of the digital euro now. In summary, the GDPR is an ambitious effort in the data protection.

Financial data and financial privacy

In the context of the GDPR and financial data, personal data concerning the digital euro includes direct personal information, transactional data, and access credentials. While money

itself is not typically classified as data, the movement of money can reveal significant information. Transactional data discloses information about personal life and behavior, through a timestamp of the transaction, a description of the purchase and the amount (Westermeier, 2020, p. 2051). These pieces of information could reveal a person's health, income, employment status, marital status, lifestyle, hobbies and more (Sharman, 2009, p. 719; Politou et al., 2019, p. 310). Privacy concerns are not limited to government surveillance; they also involve other parties, such as shopkeepers. For instance, a transaction might inadvertently reveal that a buyer is wealthy or has a medical condition (Kahn, 2018, p. 338). The prohibition of the disclosure of financial data is referred to as financial privacy (Wenker, 2022, p. 356).

2.1.3. Anti-money laundering and counter financing of terrorism (AML/CFT)

Hypothetically, if all financial data would be anonymous, the risk of personal data being exposed would be effectively zero. However, that isn't exactly a realistic scenario. In the first place because the traditional banking system is dependent on the identification of end users in order to operate the system, making anonymity incompatible with the requirements of the system. And secondly, in the application of privacy and data protection on money, there is an purposely imposed limit to what these rights entail, because anonymous payments enable criminal activity (Mahari, Hardjono & Pentland, 2022, p. 58). While banks need to comply with GDPR, they also are obliged to enforce anti-money laundering and countering the financing of terrorism (AML/CFT). Shehu (2012, p. 313) describes AML/CFT measures as "mechanisms put in place to facilitate an effective intermediation role of financial institutions, protect the integrity and soundness of the financial system, and ensure that only genuine economic activities are undertaken to promote economic growth and development". These controls cover a wide range of illegal activities, including cigarette smuggling, corruption involving high-level officials, and the financing of terrorism (Levi & Reuter, 2006, p. 290). EU's directive on AML (European Union, 2018) obliges member states to enforce AML with financial institutions. Since money leaves data trails, any form of potential criminal activity can be detected by the bank. To carry out these measures, financial institutions need to assess risks and monitor customers, requiring information on the personal data of customers, through identification and verification. Some critics see AML/CFT legislation as a justification of government intrusion into private affairs of its citizens (De Dios, 2015, p. 509). However,

privacy and data protection are not absolute rights; exceptions can be made for purposes such as criminal investigations like AML/CFT, provided that such measures are lawful, necessary, and proportionate (Politou et al., 2019, p. 311). Interesting to note is that KYC and AML measures are not aimed at the criminals, but at the commercial bank or other financial intermediaries. Even though the criminals are involved in illicit affairs, the responsibility lies with the intermediaries to detect this activity (Lastra & Allen, 2018, p. 37). This means that the private digital currencies, such as cryptocurrencies, could facilitate criminal activity by disintermediating banks, since they don't fall under the AML directive.

2.2. Cybersecurity

There is a broad digitization trend affecting all aspects of life, including money. This comprehensive digitization is rooted in the concept of cyberspace, described as a "fusion of all communication networks, databases, and sources of information into a vast, tangled, and diverse blanket of electronic interchange" (Cavelty, 2013, p. 108). Cyberspace has enabled various information systems that influence our daily lives and has made the creation of virtual currencies possible. This section will discuss various definitions of cybersecurity and cyber risk.

Privacy and cybersecurity are related in the sense that both concern personal data. Cybersecurity includes practical measures to protect information, networks, and data against internal or external threats (Li & Liu, 2021, p. 8181). There is a distinction between internal and external threats. Internal threats can be caused either intentionally (e.g. insider threat) or unintentionally (e.g. accidental disclosure of information by an employee or a third party) (Cheng, Liu & Yao, 2017, p. 1). On the other hand, external threats are often intentional. About the meaning of threats, Boeckl et al. (2019, p. 5) argue that threats are the exploitation of vulnerabilities by threat actors to compromise the CIA of devices or data. The definitions by Li and Liu (2021) and Boeckl et al. (2019) both concern the protection of information, while Carr expands on the connection between privacy and cybersecurity by explicitly mentioning personal data in her definition: "cybersecurity extends beyond protecting personal data; it encompasses the integrity of personal privacy online, the security of critical infrastructure, electronic commerce, military threats, and the protection of intellectual property" (Carr, 2016, p. 49-50). The broad and diverse topics of this definition shows a depth that distinguishes cybersecurity from information security, where cybersecurity secures

cyberspace as a whole and information security only considers data (Van Solms & Van Niekerk, 2013, p. 101).

2.2.1. Cyber risk

Providing an accurate definition of cyber risk is challenging due to the interdependence of incidents and the lack of a precise definition of cyber incidents (Aldasoro et al., 2020, p. 376; Strupczewski, 2021, p. 5). There are several scholars that have attempted to define cyber risk. The European Systemic Risk Board (ERSB, 2020, p. 9) defines cyber risk as "the combination of the probability of cyber incidents occurring and their impact" in which a cyber incident is portrayed as "a cyber event that jeopardize the cyber security of an information system or the information the system processes, stores or transmits." Cyber and related IT risks are a subset of operational risks and often described as a prominent threat to the financial system (Aldasoro et al., 2020, p. 376). Cebula and Young (2010, p. 13) also describe cyber risks as operational risks aligning with the CIA-triad. Van den Berg et al. (2015, p. 3) describe cyber risks as IT-dependent risks encountered by all actors in various cyber sub-domains during cyber activities. Similarly, Biener (2015, p. 132) highlights that cyber risk encompasses multiple sources affecting a firm's information and technology assets. Where Van den Berg et al. focus on the target, Biener focuses on the actor. Vucinic (2022, p. 43) notes that cyber risk generally refers to "the risk of financial loss, disruption, or reputational damage to an organization resulting from the failure of its IT systems" to which Florackis et al. (2023, p. 351) add that these risks are caused by external attacks.
These definitions of cyber risk share a lot of the same components and generally speak of a negative event. This is reflected in the term "risk", which the Cambridge Dictionary (Cambridge University Press, n.d.) defines as "the possibility of something bad happening". The concept of risk is broad and multifaceted, used across various disciplines and in everyday conversations. Risk is often seen as a potential future danger that can only be partially foreseen (Gellert, 2018, p. 280). Or as Adam & Van Loon (2000, p. 2) state, "the essence of risk is not that it is happening, but that it might be happening". Ulrich Beck theory of "risk society" (1992) posits that modern society is increasingly occupied with managing the risks that society produces itself. With cyberspace continually growing together with both its benefits and challenges, cyber risk is a clear example of Beck's theory. Cyber risk is complex and costly due to uncertainties and constant development. That's why risk management is not

about eliminating risk, rather about keeping risk to acceptable levels (Van den Berg, Prins & Kuipers, 2021, p. 8).

Privacy risk and cyber risk overlap

Applying the concepts established above, privacy risk in the context of the digital euro is the likelihood and potential impact of compromised privacy resulting from data processing activities or breaches in cybersecurity. This type of risk intersects with cyber risk, particularly within the framework of the CIA-triad. As Bambauer (2013, p. 669) points out, security measures define the privacy choices that can be implemented. Thus, in the case of the digital euro, cybersecurity is a critical determinant of privacy outcomes.

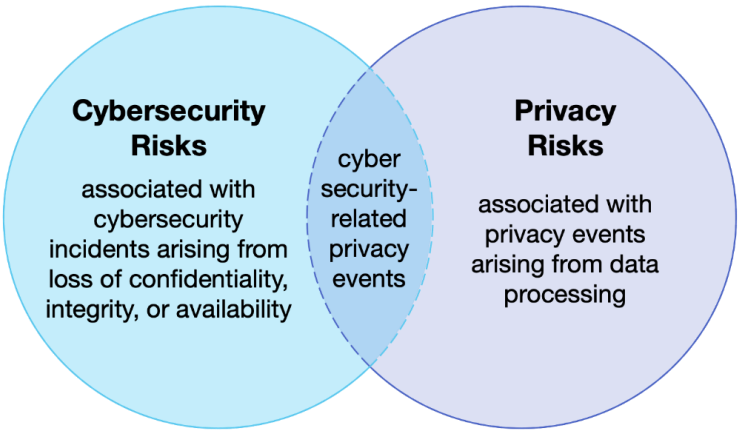

Figure 1: NIST (n.d.).

2.3. Cybercrime

A part of cybersecurity is protection from external threats. In the assessment of cybersecurity measures, inspecting the threats and origins could provide helpful by gathering information on who commits cybercrime and why and how. Gordon and Ford (2006, p. 14) argue that the term cybercrime should be deleted from the vocabulary, since criminals will utilize all methods available without regard to whether something is cyber or not. Still, they define cybercrime as "any crime that is facilitated or committed using a computer, network, or hardware device" (Gordon & Ford, 2006, p. 14).

2.3.1. Actor

According to BIS (2023, p. 38) there are various potential cybercriminal actors, including nation state-sponsored groups, criminal organizations, and insiders. Cybersecuritybeeld

Nederland (NCSC, 2015, p. 32) adds hacktivists, terrorists and cyber vandals to this list. It is difficult to assess who is behind a cyberattack due to its anonymous character and it's complicated even further due to the fact that interests overlap and there is cooperation between actors (NCSC, 2015, p. 28). The BIS and CSBN report focuses on the identity of the actor, while a more recent Cyber Security Assessment Netherlands 2021 considers the role of the actor. The Cyber Security Assessment Netherlands 2021 (NCSC 2021, p. 27-28) distinguishes between cybercriminal service providers, dependent perpetrators and autonomous groups. These three roles illustrate a cybercriminal ecosystem in which there is a market where products and services are traded and this ecosystem again displays a high level of cooperation. This crime-as-a-service enables a whole new layer of cybercrime to the picture where technical skill is no longer necessary (Europol, 2023a, p. 6). This development is also caused by generative AI tools such as ChatGPT, providing criminals with malicious code to help them with their work (Europol, 2023b, p. 8). In conclusion, looking at the threat actor can help in assessing a cyber threat, but the concealment behind cyberspace complicates determining the identity of the actor. However, an understanding of the developments in the cybercriminal ecosystem reveals that the amount of cybercrime actors is currently at a rising peak and requires a similar response from cybersecurity.

2.3.2. Motivation

A second dimension of cybercrime is assessing why cybercrime actors commit their crime. The ENISA Threat Landscape 2023 (ENISA, 2023, p. 17) recognizes the following motivations: financial gain, espionage, disruption, destruction, ideological. Financial gain is often the main motivation for cyber criminals (Ambore et al., 2017, p. 202; NCSC, 2021, p. 27). However, the main source of financial gain is by selling stolen data, rather than stealing money directly (Zhang et al., 2022, p. 418). Financial organizations are attractive targets for criminals, since they contain a vast amount of valuable data and open up the possibility for fraudulent activities (BIS, 2023, p. 38). Paying attention to the motivations of cybercriminals assists discovering what the vulnerabilities are. It is clear that the data of financial institutions is a popular target, thus putting privacy at risk, and deserves extra awareness.

2.3.3. Method

After indicating who commits a crime and why, a third way of assessing cybercrime is by determining how. This section describes what methods are used to breach a system or to gain

unauthorized access to a system. Where an understanding of the actor and its goals are helpful in assessing which sectors are targeted and vulnerable, the deployed methods decide which security measures should be implemented. First, the challenges of assessing cybercrime are discussed. Then, two broader distinctions help provide a more general understanding of used methods in cybercrime.

Challenges of assessing cyberattacks

First, the vast variety of attack types makes it impossible to account for all threats. A McKinsey report (Hasham, Joshi & Mikkelsen, 2019) notes that while categories provide an understanding, designing comprehensive categories is nearly impossible. Therefore, it might be more effective to focus on universal security measures that address multiple attack types.. Second, the concept of the cyber kill chain calls for a holistic approach (Yadav & Rao, 2015; Assante & Lee, 2015, p. 20). Cyberattacks typically exploit both human and technical vulnerabilities across multiple stages. For example, planting malware could involve technical hacking or social engineering techniques, such as scareware (Shahzad & Lavesson, 2011, p. 1). Later stages might involve ransomware, where the attacker encrypts a victim's data and demands payment to decrypt it (Europol, 2023a, p. 8). Since techniques can be used at different stages of an attack, categorization becomes difficult, and a holistic approach that considers the entire attack sequence is essential. Finally, with the digital euro being a novel technology, not all cyber threats are known. Galinec and Steingartner (2017) describe three layers of cyber threats: known knowns, known unknowns, and unknown unknowns. Known knowns are documented threats addressed by established practices, while known unknowns are risks we anticipate but lack full information about. The most challenging are unknown unknowns, which are risks that emerge from unexpected sources.

Cyber-dependent versus cyber-assisted cybercrime.

This classification of cybercrime by Wall (2007) builds on the idea that cyberspace transformed crime to varying extents of cybercrime. By taking technology and the Internet out of the equation, it becomes clear how technology has transformed crime (Wall, 2017, p. 8). Some crimes transform immensely, others wouldn't even exist without technology and the Internet. On the one hand, Wall (2007) states that cyber-dependent crimes are offenses that cannot be committed without cyberspace. These are crimes that are relatively new and had no existence before networked internet technologies, for example hacking, spam and malware (McGuire & Dowling, 2023, p. 5). On the other hand, there are cyber-enabled crimes, which

are the integration of traditional crimes and networked technologies (Wall, 2007). Including most types of fraud, cyber-enabled crimes are existent traditional crimes which have increased through the Internet and technology. If cyberspace would not exist, the crimes would still exist, but locally and at a smaller scale (Wall, 2017, p.8).

Exploiting technical vulnerabilities versus exploiting human vulnerabilities.

This dichotomy is based on the consensus in cybersecurity literature, that cyber criminals will exploit the weakest link in cybersecurity, which are humans (Sasse & Flechais, 2005, p. 14; Conteh & Schmick, 2021, p. 32). Traditionally, cybersecurity focused on the technical aspect, trying to exploit vulnerabilities existing in hardware, firmware, software application, network, and the process (Ocaka, 2022, p. 4). Cyber criminals can brute force their way into unauthorized access by trying passwords. A distributed denial-of-service (DDoS) attack could paralyze systems by disrupting connectivity through exhaustion of resources like bandwidth, memory capacity and CPU processing power (Singh & Gupta, 2022, p. 1-2). These methods exploit technical vulnerabilities.

On the other hand, humans are the weakest link. Even in the case of an extensive array of technical security measures, perfect cybersecurity can't prevent authorized access, since security mechanisms are only effective when used correctly (Whitten & Tygar, 1998, p. 3). This is partly because security is secondary to users' primary tasks in cyber activities (Pfleeger & Caputo, 2012, p. 602; Moustafa, Bello & Maurushat, 2021, p. 3). Cybercriminals know that human behavior is susceptible to social engineering, which is used to manipulate human behavior by exploiting "greed, fear, haste, gullibility" (Leonov et al., 2021, p. 471). Exploiting technical vulnerabilities requires some technical skill and the success rate of technical attacks has been minimized (Leonov et al. 2021, p. 471). These challenges are bypassed with social engineering, like phishing, which is a tactic that employs deceptive methods to trick individuals into revealing sensitive or personal information, which can then be exploited for fraudulent activities (Europol, 2023a, p. 7).

2.4. Conceptualizing Cyberspace in Three Layers

This research uses the conceptualization of Van den Berg et al. (2015) to categorize cyberspace into three layers: the technical, the socio-technical, and the governance layer. Traditionally, cyberspace was considered pure technical, but according to Van den Berg et al. (2015) the implications of cyberspace play out on these three layers. This also means that

digital euro vulnerabilities and risks can be mapped across these three layers, providing a holistic approach.

The technical layer focuses on the TCP/IP protocol stack and assesses technical cybersecurity risks, such as data breaches, within the digital euro system. With increased complexity and dependence on IT, a deeper understanding is demanded (Van den Berg et al., 2015, p. 3). Cyber-dependent crimes are tied to the technical layer and exploit technical vulnerabilities within the system, such as hacking, malware, and DDoS attacks, which directly target the technical layer of cyberspace. The technical layer, therefore, is the foundation where such threats are most likely to occur. However, the consequences of the first layer often play out in the socio-technical layer. This layer discusses the complex interaction between human activity in cyberspace and data storage and processing systems (Van den Berg et al., 2015, p. 2). Exploiting human vulnerabilities falls within the socio-technical layer and cyber-enabled falls under both the technical and socio-technical layers. Here, the focus is on how human actions can compromise security, even when the technical systems are well-protected. Finally, the governance layer encompasses the management of the technical and socio-technical layers by various human actors and organizations (Van den Berg et al., 2015, p. 2). It ensures that the right regulations, such as GDPR, are in place to manage the technical and human vulnerabilities. By understanding and addressing vulnerabilities across the technical, socio-technical, and governance layer, the digital euro can enjoy a better cybersecurity.

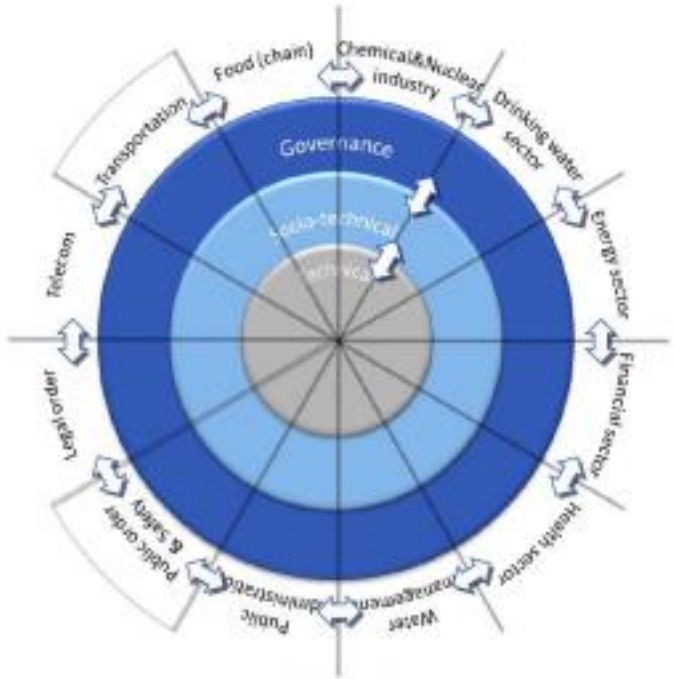

Figure 2: Van den Berg et al. (2015, p. 2).

2.5. Conclusion

In this chapter, a theoretical framework with the concepts of privacy, cybersecurity and risk is established. According to the GDPR, it is the responsibility of the relevant actors, the ECB and the intermediaries, to safeguard the personal data of the end users of the digital euro. This research focuses on cybersecurity threats with intentional unauthorized access. While important, a research on data breaches through authorized access requires a whole other scope than this thesis. For example, internal threats are often unintentional. Intentional threats pertain to security, while unintentional threats relate to safety; however, these concepts are interrelated (Van den Berg, Prins & Kuipers, 2021, p. 9). A similar case can be made for internal and external cybersecurity.

3. Understanding Central Bank Digital Currencies (CBDCs)

The digital euro is currently in its development phase, and the European Central Bank (ECB) is not alone in this endeavor. Already in 2020, approximately 80% of central banks worldwide are involved in research, experimentation, or development of CBDCs (BIS, 2020a, p. 3). One of the first mentions of CBDC was in 2015, when the Bank of England put forward the idea of issuing a digital currency (Bank of England, 2015, p. 6). Although CBDCs are a relatively new phenomenon, a comparable goal was introduced decades ago by Tobin (1987, p. 13), who envisioned a "medium with the convenience of deposits and the safety of currency." This would be a currency that enables online payments like in the commercial banking system, but with a guarantee by the central bank. The CBDC aims at achieving exactly that.

3.1.1. Defining CBDC

Defining CBDC is challenging because the term encompasses various concepts and designs (BIS, 2018). While CBDCs share similarities with other forms of money and other CBDCs, they differ significantly due to their unique designs, legal contexts, and the objectives of the issuing central banks. The International Monetary Fund (IMF) defines CBDC as a "digital representation of a sovereign currency issued by and as a liability of a jurisdiction's central bank or other monetary authority" (Kiff et al., 2020, p. 13). Unlike the current financial system, where commercial banks operate under control of the central bank, a pure CBDC

system would have the central bank overseeing the entire currency circulation on its own (Chu et al., 2022, p. 2).

Despite the complexities in defining CBDC, there is a general consensus in the literature on certain key aspects: CBDCs are digital, and they are issued by a central bank (Bindseil, 2019, p. 2; Davoodalhosseini, 2022, p. 3; Ward & Rochemont, 2019, p. 3; Agur, Ari & Dell'Ariccia, 2022, p. 62). This distinguishes CBDCs from crypto assets, commercial bank money, and cash. These distinctions are made clear in the Venn diagram by Cœuré and Loh (BIS, 2018) that is based on Bech and Garratt (BIS, 2017, p. 55) in figure 4. The four features of the money flower are: technology (account-based or token-based), issuer (central bank or other), form (electronic or digital), accessibility (universal or limited). The money flower illustrates how these distinctions demonstrates different types of money and to what extent they share similarities. The diagram also shows that a CBDC can have varying characteristics. General purpose digital central bank money, both account-based and token-based, is widely accessible to the public and is referred to as retail. Digital central bank money inaccessible to the public can still be a CBDC called wholesale CBDC. Retail/wholesale and account-based/token-based represent important dichotomies in the discussion of CBDCs, which will be explored further in this thesis.

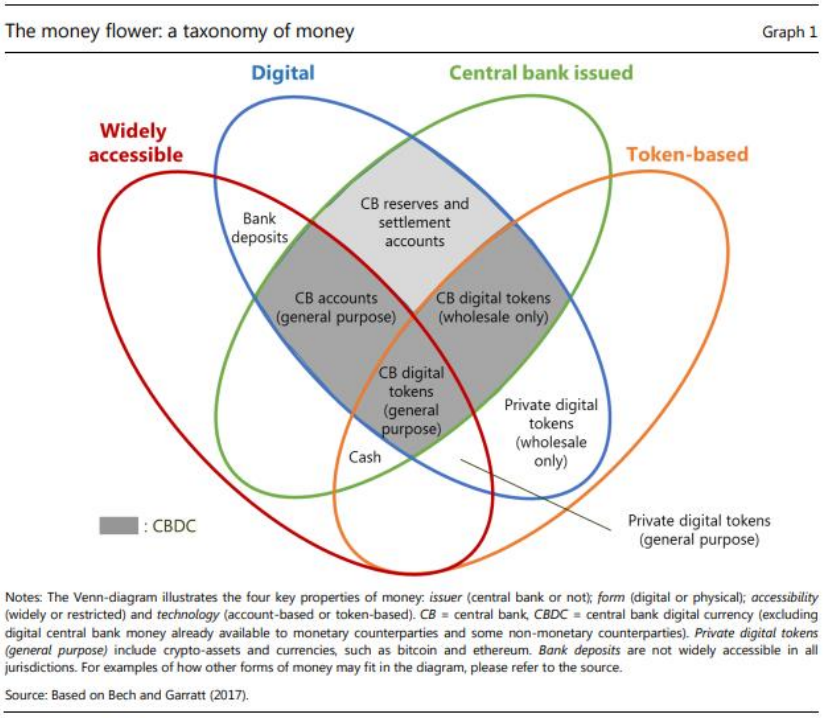

Figure 3: Cœuré and Loh (BIS, 2018, p. 5).

3.2. The rise of CBDCs

There are several key events that have driven central banks to consider issuing CBDCs. This section describes the general motivations that pushed central banks to pursue the developments of CBDCs.

3.2.1. Balancing private and public money

The primary motivation for this move can be attributed to the effort of retaining balance between public and private money (Bolt, Lubbersen & Wierts, 2022, p. 7). According to a BIS survey (2024, p. 6) on central banks, preserving public money is among the key drivers for more than two thirds of respondents. Public money is money issued by the central bank, while all money no issued by the central bank is private money. Central banks perceive threats to their monetary authority posed by competition of other forms of money: crypto assets and commercial bank money and other CBDCs.

First, cryptocurrencies only exist in cyberspace and offer a private alternative to state-issued money that is decentralized and anonymous, allowing transactions without relying on third parties (Zhang & Huang, 2021, p. 264). Over the past decade, cryptocurrencies have gained broader market acceptance and posed increasing competition to traditional currencies (Fang et al., 2022, p. 1). Central banks are concerned that these virtual currencies could undermine their ability to control monetary and macroeconomic policy, prompting many to develop their own digital currencies (Náñez et al., 2020, p. 12; Laboure et al., 2021, p. 667; Bibi & Canelli, 2023). The fear is that central banks may lose their "unique position as monopolistic supplier of cash" amidst these new monetary alternatives (Bofinger & Haas, 2020, p. 1). Monetary sovereignty is threatened when other currencies are used for pricing, wages, and financial contracts (Brunnermeier & Landau, 2022, p. 16). However, a member of the executive board of the ECB argues that CBDCs, as state-issued currencies, offer greater stability with state-backed guarantees (Panetta, 2021). Furthermore, cryptocurrencies applications tend to provide lower user privacy standards than traditional banking applications, which means higher risk for end users (Sai, Buckley & Le Gear, 2019, p. 6).

Second, commercial bank money is another form of digital money that also contributes to the diminishing monetary power of central banks. Unlike cryptocurrencies, commercial bank money is not a new phenomenon and commercial bank and central banks cooperate.

However, it is private money and the main reason for the declining use of cash, which is issued by central banks (Indrawati, 2023, p. 373; Khiaonarong & Humphrey, 2019). This trend is again driven by the digitization of money, making digital transfers more convenient than physical transactions. The COVID-19 pandemic accelerated the decline of cash usage due to concerns about physical contact, favoring digital payments (BIS, 2020b; Rennie & Steele, 2021). With the diminishing role of cash and the rise of (virtual) commercial monies, central banks face reduced control over money, a situation that CBDCs could address.

Lastly, developing a CBDC also helps prepare for potential competition from other CBDCs. As other countries develop and implement their own digital currencies, cementing a national CBDC will increase the survivability of that digital currency (BIS, 2023, p. 10). In the end, as Mbanaso and Dandaura (2015, p. 18) argue, a nation's ability to achieve sustainable growth in an information-driven economy is essential to keep up with the competition.

Until CBDCs are implemented, cash remains the only legal tender in most monetary regions. Legal tender must be accepted for payments of goods, services, or debts (Indrawati, 2023, p. 375). Despite being legal tender, cash is often inconvenient due to its physical nature, whereas commercial bank money, though easier to use, is not legal tender. Therefore, Pocher and Veneris (2022, p. 1778) argue that CBDCs occupy a middle ground between cash and commercial bank money, offering universal accessibility and robust transaction capabilities. The issue of the decreasing amount of central bank money in circulation is not always apparent to the public. According to Brunnermeier and Landau (2022, p. 19), this is the paradox of public money: people tend to view money as a whole, without distinguishing between bank deposits and cash. This confusion is supported by an ECB study on New Digital Payment Methods, where respondents indicated they did not fully understand the difference between central bank money and commercial bank money (ECB, 2022a, p. 48).

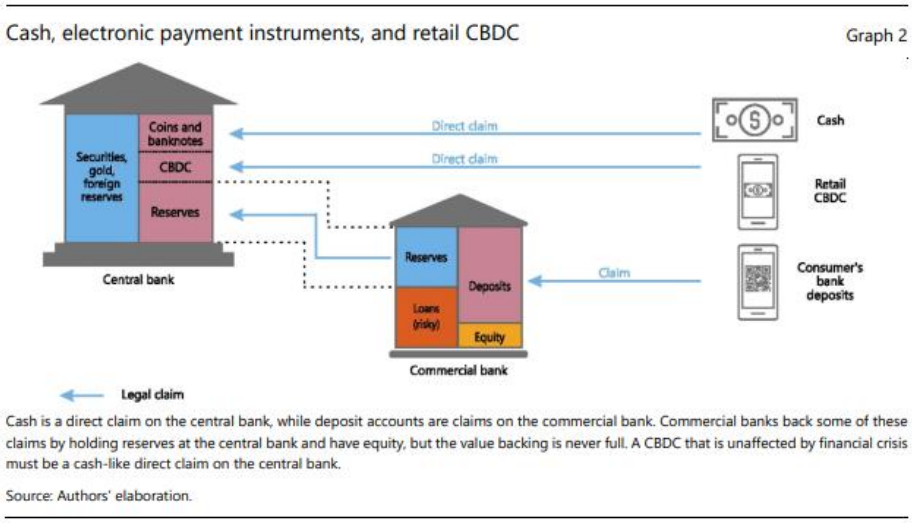

Figure 4: BIS (2021, p. 6).

3.2.2. Secondary incentives

With this envisioned universal accessibility of CBDCs, central banks promise to enhance financial inclusion by providing a secure and accessible form of money for all citizens, regardless of their access to traditional banking services (Tsang, Yang & Chen, 2022, p. 2;. Soderberg et al., 2022, p. 4; Appendino et al., 2023, p. 7). CBDCs can broaden access to the financial system, serving the unbanked and under-banked populations, who often face barriers to entering the financial mainstream. By offering a digital alternative that is universally accessible, central banks can help bridge this gap, promoting greater economic participation and inclusivity. Additionally, central banks aim to reduce more barriers as CBDCs should increase payment efficiency (Laboure et al., 2021, p. 670; BIS, 2019b, p. 8). Furthermore, some authors argue that CBDCs can play a crucial role in AML/CFT practices (Sidorenko, Shevela and Lykov, 2021; Mahari, Hardjono & Pentland, 2022). The financial sector is a critical sector vulnerable to people taking advantage of the system (Aldasoro et al., 2020, p. 347; ESRB, 2020, p. 18, Bouveret, 2018, p. 5). The traceability and transparency of digital currencies allow for better monitoring of financial transactions, making it harder for illegal activities to go undetected. Central banks are uniquely positioned to provide consumers with a method of payment that offers privacy because they can credibly commit to safeguarding data from outside vendors, unlike private sector alternatives that are bound by profit-maximization incentives (Garratt and Lee, 2018; Ahnert, Hoffman & Monnet, 2022, p. 4). However, a currency that is better than alternatives in monitoring financial behavior is unlikely to trigger an enthusiastic response by the public.

3.3. CBDC: Design choices and its implications

Not all CBDCs are created equal. Numerous design choices must be made, and as most central banks are still in the development or research phase, no universal standard exists. Also, CBDCs are different and could have varying purposes. Technically, the possibilities for finalizing a CBDC are endless. This research focuses on four main design choices as described by Bossu et al. (2020, p. 9).

First, account-based and token-based concerns the transfer mechanism and identification of the user or the verification of the CBDC. Second, wholesale and retail refers to the target audience or the customer base and the usage by this group. Third, direct and indirect related to the level of involvement by the central bank and the claim structure. Fourth, and lastly, centralized and decentralized touch on concepts as architecture and technology. This segment dives deeper in these dichotomies and nuances and explains how every design choices has its distinct implications, but also points out how the design options are heavily interlinked.

3.3.1. Account-based versus Token-based

A first distinction in CBDC design can be made in transfer mechanisms, between account-based and token-based systems. In an account-based system, users open a current account, and the payer must be identified as the account holder making the payment (Chan, 2021, p. 2). The existing commercial banking system operates on this model, providing accounts for all customers. On the other hand, central banks typically open accounts for financial institutions, non-bank financial intermediaries, and occasionally retail customers (Bouchaud et al., 2020, p. 17). A pure account-based CBDC approach would require central banks to open accounts for all users, significantly increasing their operational scope. This design is technically challenging, since central banks generally lack the expertise and experience (Passacantando, 2021, p. 121; Tsang, Yang & Chen, 2022, p. 7). This central banks' inexperience concerning account management could provide risks to the processing of personal data. However, an account-based CBDC could also involve intermediaries to mitigate this problem, as explained in the "3.3.3. direct versus indirect" section.

Conversely, a token-based system focuses on the object, for example a (digital) coin or a voucher, being transferred rather than the account holder. The identity of the payer is irrelevant, instead the question is if the object is authentic (real or counterfeit)" (Chan, 2021,

p. 3). Armelius, Claussen, and Hull (2021, p. 7) define a token-based CBDC as a “digital object that has a given value expressed in the national unit of account and is a claim on the respective central bank." Brunnermeier and Landau (2022, p. 13) note that tokens are representations that can be both digital and physical. For example, cash is a physical token that anyone can use to make a payment without needing to prove that the payer is the actual owner of the coin or banknote. The coin or banknote itself at that moment is enough to conclude a payment. Accordingly, "cash-like CBDC" typically refers to token-based CBDCs, which are stored in electronic wallets and enable anonymous, peer-to-peer payments (Bofinger & Haas, 2020, p. 11). The difference between electronic wallets and accounts can be confusing, since the term account is used for varying purposes. In this context, wallets refers to front-end user interfaces, for example a bank application, and accounts relate to the account balances in the central banks’ back-end databases.

In an account-based model there is no object providing value in itself. Payments often involve a card or mobile phone that is used to make contact to the bank’s account ledger, its database. Phones and cards do have value, but instead of giving away them away for their inherent value, they are used to verify the account owner and to indicate that there is enough credit on the account to make a transaction. A key difference between account-based and token-based CBDCs is that token transfers do not require reconciling databases. During a transaction in an account-based system, the payer’s database contacts the ledger in order to verify the payer. Since token-based system doesn’t require this verification in transactions, contacting the ledger is not necessary, enabling decentralized peer to peer payments (Chan, 2021, p. 7). Furthermore, tokens need a personal identity to function, but do require some ownership. The ownership of a digital token lies in the access to the token (e.g. private cryptographic key), rather than the possession. Tokens can represent a direct transfer of ownership without involving a third party, reducing privacy risks (Bouchaud et al., 2020, p. 17). The lesser the amount of parties involved, the smaller the data trail and the smaller the potential data points susceptible to cyberattacks. Furthermore, apart from pure account-based and token-based models, hybrid models also exist. For example, Sweden's Riksbank pilot CBDC is account-based but includes low-value token-based prepaid cards (BIS, 2020b, p. 28). Similarly, the Chinese e-CNY can be described as semi-account-based; it must be stored in an application or device linked to an account, but the token can be separated from the account, and the device can be separated from the user (Xu, 2022, p. 242).

Online versus offline

Because token-based payments don't require access to the ledger, they can be made both online and offline, as opposed to account-based transfers, which require an internet connection (Chu et al., 2022). According to a BIS survey (BIS Innovation Hub, 2023a, p. 13), 49% of central banks consider offline payments "vital" in retail CBDC and another 49% of central banks deem offline payments "advantageous". There are a few reasons why central banks are this interested in offline payments. First, as mentioned, offline payments provide more privacy than online payments. Cash-like CBDC implies that its anonymity level is equal to that of cash. The anonymity of paper currency protects individuals from the risk of misuse of payment information by the state, whether democratic or dictatorial (Masciandaro, 2018, p. 541). However, since CBDCs are digital and need to be documented in some way in order to function, it can never be as anonymous as cash (Mu & Mu, 2022, p. 18; Tsang, Yang & Chen, 2022, p. 9; Bofinger & Haas, 2020, p. 20). Second, online systems rely on the central ledger being permanently up and accessible (Urbinati et al., 2021, p. 62). Offline CBDC could enhance system resilience during outages of the online CBDC system or network infrastructure failures (BIS Innovation Hub, 2023b, p. 10). It is particularly beneficial as a backup option in cases of unreliable online connectivity. Third, where CBDCs in general are intended to foster financial inclusion, offline payments could take this a step further by including people without internet connection.

3.3.2. Wholesale versus Retail

Different CBDCs caters to different target audiences. Wholesale CBDCs are issued for financial institutions and clearinghouses. Since wholesale payments do not benefit from cash-like anonymity, the benefits of CBDCs in wholesale payments include improving efficiency and reducing costs (BIS, 2017, p. 56-57). Some central banks already issue a wholesale digital currency, such as the EU's TARGET2, which is an account-based real-time gross settlements (RTGS) system. This is an interbank system, which is no CBDC, but you could argue it is, since it is electronic and central bank issued (Lannquist, Warren & Samans, 2020, p. 8). Wholesale CBDC may also become token-based using a decentralized ledger (BIS, 2019a). This research, however, focuses on retail CBDC, because digital euro end users don't have access to wholesale CBDC.

Retail CBDCs are designed for peer-to-peer (P2P) and person-to-business (P2B) payments (Sethaput & Innet, 2023, p. 2185; Lee, Yan & Wang, 2021). Most CBDC explorations focus on retail CBDCs, which are intended for the general public. Retail CBDC is the solution to the framed problem that central bank money usage is declining, by offering a currency that is universally accessible, electronic, and central bank issued (Bjerg, 2017, p. 24). The retail sector has a large consumers base, consisting of individual end users and merchants, and a CBDC would need to cater to the varying needs. These needs differ from wholesale CBDC. For example, proximity payments only serves retail payments and accordingly paying with card, wearable or something comparable. Since retail CBDC involves a much higher limit of actors than wholesale CBDC, the amount of cybercrime targets and consequential cyber privacy risks are accordingly high.

3.3.3. Direct versus Indirect

Direct versus indirect concerns topics such as user interaction and the level of involvement of central banks in the CBDC payment system. Direct CBDCs are issued and fully managed by the central bank, described as a one-tier or one-layered system (Pocher & Veneris, 2022). Soderberg et al. (2022) refer to this as a "unilateral CBDC," where the central bank performs all functions within the system. Since central banks are not used to this, the probability of direct CBDC implementation highly depends on context. Populations with high geographic dispersion and largely unbanked, such as the Bahamas, are more likely to adopt a direct model (Lloyd, 2020, p. 90).

Indirect CBDCs are issued by central banks but distributed via commercial banks or other PSPs. The involvement of intermediaries makes indirect CBDCs a two-tier or multi-tier design, alike to traditional banking (Lee, Yan & Wang, 2021, p. 5). In this CBDC model, intermediaries play a role in the onboarding process, responsible for performing know-your-customer (KYC) checks, ensuring compliance with regulatory requirements, and handling consumers' payments in real-time. Meanwhile, the central bank maintains oversight by periodically recording retail balances (BIS, 2023). An indirect CBDC is not only different from direct CBDC in the sense that central banks don't run the whole system, also important is the fact that there is no direct claim of the account holder on the central bank (Lloyd, 2020, p. 90). This means that the intermediary carries the risk and is responsible for fulfilling the claim, bringing down the argument by central banks that CBDC qualifies as a risk-free

guaranteed currency. According to Bossu et al. (2020, p. 10), "in order to qualify as a real CBDC, it needs to be a liability of the central bank, not a commercial bank." This problem is fixed with hybrid CBDC, providing a direct claim on the central bank, while intermediaries operate the system (BIS, 2020c, p. 88). Additionally, the central bank must have the technical capability to restore and transfer retail CBDC holdings during technical failures by keeping a copy of all retail balances (Lloyd, 2020, p. 90).

3.3.4. Centralized versus Decentralized

Lastly, centralized and decentralized describe the control architecture and its technology of the CBDC. The comparison between CBDC and private digital currencies, such as Bitcoin, finds its origin in this dichotomy. An explanation of the double spending problem is required for this section. The possession of the cash is viewed as a proof of ownership since each coin or banknote has a unique physical existence (Chan, 2021, p. 4). On the other hand, any digital representation of anything for that matter, such as digital currencies, are easily created and reproduced (Dwyer, 2019, p. 81; Chan, 2021, p. 7). This means that the same bit of money could be spend several times, making the currency worthless. Furthermore, the payee has to believe that the payer has sufficient funds to make the transfer. In contrast to cash, the receiving party has no way of knowing this. A way of solving this problem is external validation by recording all transactions on a ledger. A ledger is an “authoritative set of records collectively held by a significant proportion of network participants at any point in time, such that records are unlikely to be erased or amended (i.e. ‘final’)” (Rauchs et al., 2018, p. 25). Once the transaction is confirmed and recorded on the ledger, it is validated and secure, providing both parties with confidence and trust in its finality. A key point in this definition of ledger is “significant proportion of network participants”, describing who is in control of the ledger. This could be a single entity, in a centralized system, or multiple entities, in a decentralized system, as long as these entities control a “significant proportion”.

In a centralized system, there is one trusted third party that controls one ledger where all transactions are more is stored (Sethaput & Innet, 2023, p. 2190). In the current commercial bank system, each commercial bank has a ledger containing the information of its clients. Apart from validating payments, the ledger is useful in case of a claim of an incorrect payment, so the bank can check and reverse the payment. Also, the information on the ledger is used in AML/CFT enforcement. In a centralized ledger, all the data is in the hands of one

entity creating a single point of failure, laying out an interesting target for cybercriminals (Wylde et al., 2022, p. 8).

In a decentralized system, multiple entities often have access the same replicated ledger (Rauchs et al., 2018, p. 45). A decentralized system operates across multiple centers, increasing robustness and reducing the risk of total system failure if one center malfunctions (Rahman, 2020, p. 6). However, this doesn't reduce the privacy risks; in fact, it increases the risk. When literature refers to decentralized, more often than not, it is about distributed.

To combat these issues by omitting a third party entirely, distributed systems have emerged. Conveniently after the financial crisis of 2008, with people's trust in the banking system at an all-time low, a certain "Satoshi Nakamoto" released a white paper about Bitcoin (Yermack, 2024, p. 36). Nakamoto (2008, p. 1) aimed to create a system that was based on proof, rather than trust, and created a payment mechanism over a communications channel without the need of a trusted third party. These decentralized systems utilize Distributed Ledger Technology (DLT), such as blockchain, which does not rely on a central authority, but uses a consensus algorithm to ensure integrity and consistency (Zouina & Outtaj, 2019, p. 3). No single entity controls the blockchain, but instead, is maintained by a network of nodes. Blockchain validates transactions through cryptography, while the ledger serves as a public transaction record. Although data is secured through cryptography, the blockchain is permissionless, meaning that it is visible for all participants, making it highly transparent. Other permissioned DLTs are limited to selective participation to prevent full transparency (McLean & Deane-Johns, 2016, p. 97; Rennie & Steele, 2021, p. 13).

In the beginning, CBDC was envisioned to be based on DLT (Broadbent, 2016; BIS, 2017). There are examples of CBDC using DLT: the Bahama's (Wenker, 2022), China and Sweden (Sethaput & Innet, 2023). However, while distributed systems are highly reliable, they are also complex and face scalability issues, making them less suitable for the high transaction volumes expected of a CBDC (Xu, 2022, p. 236). Also, there is no widely accepted cybersecurity framework for DLT, since the vulnerabilities are not yet fully understood (BIS, 2023, p. 53). Furthermore, there are potential governance concerns if maintenance and supervision responsibilities are not centrally established (Laboure et al. 2021, p. 670).

3.4. Conclusion

This chapter provided a brief overview of the definition and emergence of CBDCs. Furthermore, it showed to what extent CBDC can vary and how different design implementations affect privacy and data protection. Some design options are inherently more private and secure, but are sometimes harder to implement. These four dichotomies help in placing a CBDC in a bigger context, but other aspects also play an important role. For example, the devices used in transactions influence the cybersecurity and accordingly privacy heavily.

4. Methodology

In this section, the focus and the scope of the research are defined, along with the methodological choices made to achieve the study's objectives. Additionally, this section outlines data collection methods, case selection criteria, and the study's limitations.

The research is a case study focusing on the digital euro emerging in the European financial landscape. Both the online and offline implementation of the digital euro are researched. The CBDC of the ECB is chosen as the central focus due to the EU's prominent role as a global advocate and frontrunner in privacy rights. The ECB's transparency and regular updates make it an ideal subject for analysis. Furthermore, given the EU's influential regulatory framework, as described by Anu Bradford's concept of the Brussels Effect (Bradford, 2020), the digital euro has the potential to shape international standards for CBDCs.

Research Question

This qualitative study aims to map the cyber privacy risks of end users associated with the potential implementation of the digital euro. In order to gain a conceptual grasp of what the digital euro might entail, the theoretical framework is applied to the case. Then, the case is compared to the existing forms of money in the current financial landscape. The research question guiding this thesis is:

"How do the cyber privacy risks for end users of the digital euro in both its online and offline implementations compare to existing forms of money, such as cash and commercial bank money?"

Data collection

The data for this research is sourced exclusively from publicly available literature. Search engines like Google Scholar and the Universiteit Leiden library catalog were utilized to gather academic literature to inform the theoretical framework. Since CBDC is a multidisciplinary concept, a crash course on economics, finance and crypto technology (consisting of lectures on YouTube, reading books and articles) was needed to fully grasp the concept of CBDC and being able to place it in its relevant contexts. Additionally, reports and documents from the ECB and EU were sourced through general internet searches to ensure a balanced representation of academic and professional perspectives. After, more specific search terms such as “privacy”, “cybersecurity”, “risk” and “central bank digital currencies” where used, often in combination with each other. Further research was conducted when new relevant reports were published. In this way, the conducted research started off with desk research on the background of the topic over the course of several months in the beginning of 2024. As the research progressed, new articles were published with information that sometimes rendered previous statements borderline untrue. Although it is wise to limit a research within a strict time scheme to avoid this problem, the author couldn’t resist including the most recently published articles and reports in this thesis. As a result, this research consisted of continuously alternating between desk research and writing all the way to the end of the process. Also, since the ECB continuously publishes reports, the information about the digital euro is scattered across the array of publications and requires attentive interpretation to connect the dots. This research considers all relevant ECB publications about the digital euro, covering multiple phases of development,

Scope

Before the analysis, this research requires some clarifications on the scope and concepts. Geographically speaking, this research is limited to EU residents, since that group is the ECB’s target audience. The study specifically addresses end users' cyber privacy risks, as these individuals represent the most vulnerable point in cybersecurity systems (Dawson & Thomson, 2018, p. 8). In this research, that means end user residing in the euro area, the group of states that use the euro as currency. The first release of the digital euro focuses solely on euro area residents, while subsequent releases include other EU-member states and even third countries (ECB, 2022c, p. 6). Merchants could be classified as end users, but this research focuses on consumers only. The analysis does not differentiate between types of end users or the effects of data breaches on different user groups. The focus is on vulnerabilities

and the risks associated with personal data, particularly in the context of cyberattacks. Although the study examines cyber threats, it does not quantify their impacts. The emphasis is on the design aspects that provide end users with relative agency and the potential for significant change, such as token-based offline payments, which are elaborated upon in the data analysis section.

According to the proposal, the digital euro will be available to natural and legal persons residing or established in EU Member States whose currency is the euro, as well as to those who opened a digital euro account while in these states but have since relocated. Visitors may also access the digital euro under specific conditions (European Commission, 2023a, art. 13). Payment service providers can distribute the digital euro to individuals or entities in Member States whose currency is not the euro only if an arrangement has been signed between the European Central Bank and the national central bank of the respective state (European Commission, 2023a, art. 18). Furthermore, distribution to persons in third countries is permissible only if the European Union and the concerned third country have established a prior agreement (European Commission, 2023a, art. 19).

5. Findings

This chapter applies the theoretical framework to the case of the digital euro. The theoretical framework provided a conceptual foundation of cybersecurity privacy risks, an understanding of CBDCs in the financial landscape and an overview of potential CBDC implementations based on the variation of design choices. This chapter starts with an introduction on the digital euro, narrating its emergence and development process. Then, the digital euro will be evaluated in terms of design choices according to what is known at this moment in time.

5.1. The emergence of the digital euro

As early as 2018, Benoît Cœuré, a former Member of the Executive Board of the ECB, acknowledged that various central banks were researching or considering the research of CBDCs (Cœuré, 2018). By 2020, Yves Mersch, a current member of the Executive Board, confirmed that the ECB jumped on the bandwagon and was in fact one of the researching central banks (Mersch, 2020). This section outlines the ECB's exploration of the digital euro

so far and describes what drove the ECB to issue a CBDC. Furthermore, the segment sets out the expected benefits for the end user to adopt the digital euro and ends with a development planning.

Reason to issue a digital euro

There are two primary drivers for issuance mentioned in the impact assessment that accompanied the digital euro proposal (ECB, 2023b). The first driver is the increasing digitalization of the economy, which has resulted in central bank money being less relevant for payments in certain parts of the economy (European Commission, 2023b, p. 16). According to the SPACE study (ECB, 2022, p. 11), cash in the EU remains predominant for Point-of-Sale (POS) and P2P payments, but its usage is declining, particularly post-pandemic. This is in accordance with the literature on CBDC emergence. However, the ECB has repeatedly stated that the digital euro has no intention of becoming a replacement of cash. This intent is emphasized by the planned release of euro banknotes in 2026, where the theme "European culture" won the design competition with 21% (ECB, 2023e). However, even though cash won't disappear, the growth of e-commerce has accelerated the shift towards electronic payments, supported by an increase in internet access among EU households, which rose to 92% in 2021 from 72% a decade earlier (European Commission, 2023b, p. 17). The second driver concerns the competitive threat posed by foreign CBDCs and private digital currencies, which could diminish the role of the euro in the European retail market (European Commission, 2023b, p. 17). Facebook/Meta's money project Libra/Diem changed central banks' attitude towards cryptocurrencies, since the Libra/Diem challenged CBDC in all three functions of money: to function as a means of payment, a store of value, and a unit of account (European Commission, 2023b, p. 19).

These drivers translate into two core objectives for the ECB. First, the ECB aims to reinforce the euro's monetary anchor in the digital age by ensuring that central bank money, in both its physical and future digital forms, remains widely available and accepted by all euro-area residents and businesses, while also preserving financial stability. Second, the ECB seeks to strengthen the EU's strategic autonomy by enhancing the euro's competitiveness against other currencies, including third-country CBDCs and private digital currencies (European Commission, 2023b, p. 28). Again, this public money argument reflects the CBDC literature.

The ECB's reasons for issuing a digital euro might be valid and could even have direct impact on residents in the Eurosystem. However, without clear benefits it is unlikely that the digital euro gains widespread adoption. Acceptance by the public is crucial; therefore, the ECB has launched public consultations to gather feedback on the design implications of introducing a digital euro (Panetta, 2020). According to ECB press reports, there are several benefits to using the digital euro. First, the ECB emphasizes that the digital euro would be easy to use, secure, and provide strong privacy protections. Second, the ECB or the national central bank carries the risk over the digital euro, instead of a commercial bank. Third, the digital euro would enhance the financial inclusion of the EU. The digital euro is stable to the euro and is just another way of using the euro. The fact that the digital euro will also have an online variant increases the payment options even further. Lastly, the digital euro will be free of charge for basic use (ECB, 2024b, p. 11). Basic could include services in terms of account management, automated funding, transactions, provision of a payment instrument and waterfall services (ECB, 2022b, 6). What falls outside of the scope of basic use is not entirely clear. As of now, cash is also free of charge, keeping the spirit of central bank money. On the other hand, the services provided by commercial banks do have a fee.

Timeline and Development Phases

After it was confirmed that a digital euro would be issued, the ECB experimented with ideas and spoke to stakeholders to select the right approach. In October 2021, the ECB decided to continue with the project, launching the investigation phase, lasting 24 months (ECB, 2021a). During this phase, the focus was on developing a functional design based on user needs, including the use of focus groups, prototyping, and conceptual work. As of now, the ECB is in the second phase of the digital euro project. Since November 2023, the ECB entered the preparation phase, which is expected to last until 2024. This phase involves finalizing the digital euro rulebook, selecting providers for the digital euro (ECB, 2023a). In November 2025, the ECB might decide to continue one again with the project, potentially finalizing the development.

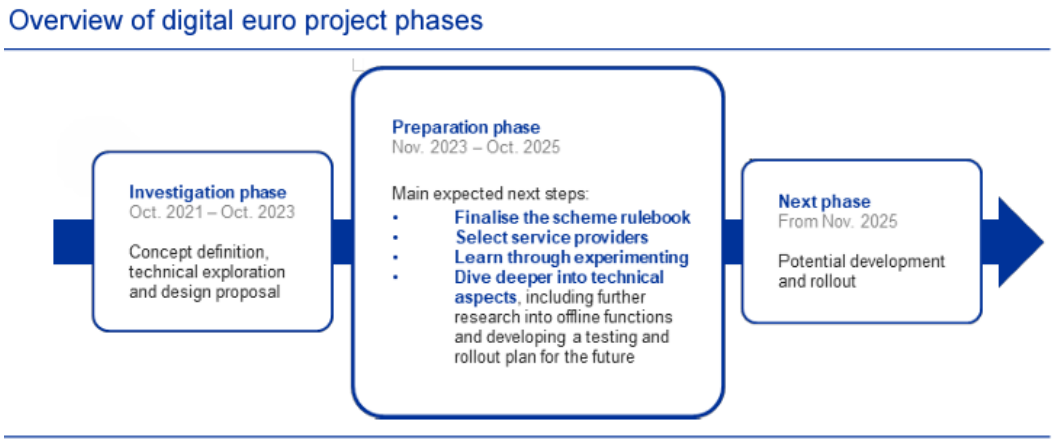

Figure 5: ECB (2024, p. 2).

The ECB continuously publishes all kinds of reports, press releases and interviews to keep the interested updated. Most useful in the analysis of design choices are the progress reports, of which there are four published; the most recent one on June 24 this year. These reports contain updates in terms of technical developments, prototypes and infrastructure.

5.2. The design choices of the digital euro and its implications

This section outlines the expected design of the digital euro based on current perspectives. The four dichotomies presented by Bossu et al. (2020) provides a framework in analyzing the digital euro. However, it proves difficult to paint the whole picture, using these four criteria, since they overlap greatly. Furthermore, this analysis isn't complete without involving payment methods and devices, which don't necessarily fall under one of the four criteria. Some aspects of the payment system finds its way on all dichotomies. For example, let's say an end user uses the digital euro app to transfer any amount of money to a friend. In this case, there is a retail transaction that is token-based and gets verified by a PSP on a centralized ledger. To fit these criteria, the narrative of this chapter first discusses retail and wholesale, which cements the goal of the digital euro and provides an overview of the use cases and form factors. Then, the second part describes the technology behind both the online and digital euro, involving account-based and token-based and centralized and decentralized. Lastly, the direct and indirect discusses how PSPs interact with the users and the system.

Given this point, the digital euro is sure to be retail and indirect, or rather hybrid. Also, it is anticipated that the digital euro will both be token-based and account-based and involve elements of both centralization and decentralization.

5.2.1. Retail versus wholesale

Out of all four criteria by Bossu et al. (2020), retail was the only choice that had no doubt. In the first place, because the Eurosystem already has a wholesale CBDC in the form of TARGET2, while there is no Eurosystem CBDC for the retail market. Secondly, one of the key drivers of the digital euro was to compete with emerging retail currencies. Furthermore, the goal is to provide the public with central bank money accessible to all citizens and businesses. Aiming at a legal tender, the digital euro is inherently retail, since legal tender should be accepted anywhere in the Eurosystem.

The retail digital euro will know three use cases, which are payment segments that a digital euro would serve. The use cases of the digital euro are as follows: P2P payments, available online and offline, e-commerce payments, available online; and POS payments, available online and offline (ECB, 2024a, p. 17). The latter of the three, POS payments, will need further research and development to provide equal security to the first two use cases, since POS terminals are not equipped with secure elements (ECB, 2024d, p. 18). The ECB even prioritizes P2P payments and e-commerce for digital euro use cases (ECB, 2022b, p. 4). This means that in the beginning the online euro can be used in P2P payments and e-commerce, while the offline digital euro will only be used in P2P payments, since e-commerce requires an internet connection and can't be a proximity payment. Likewise, POS payments won't be discussed to the same extent as P2P and e-commerce payments, but POS payments will likely correlate with proximity P2P payments. This essentially leaves three use cases in the analysis: offline P2P payments, online P2P payments, and online e-commerce payments.

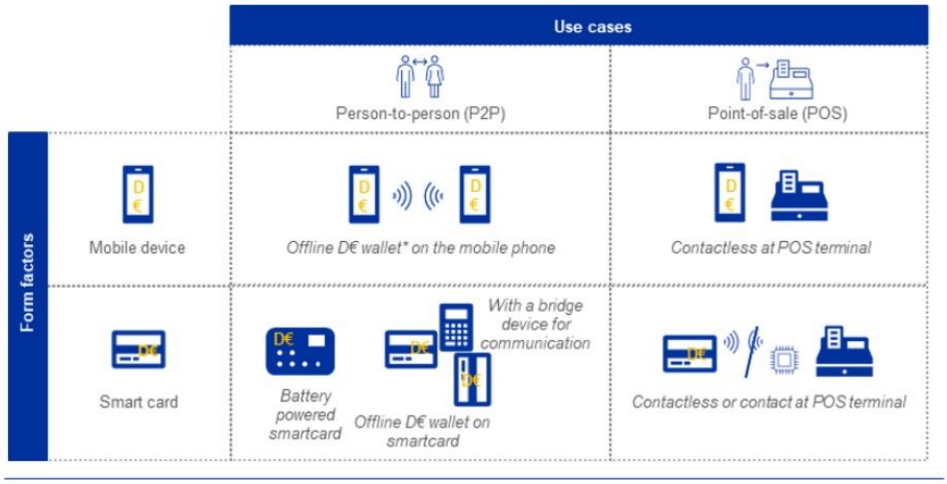

Figure 6: ECB (2024b, p. 6).

Offline use case

Where use cases showcases where the end user can make a transaction in the retail environment, the form factors depict how the payments can be made. A form factor is combination between a device and a communication technology that together support the exchange of information (ECB, 2022d, p. 7). Offline P2P speaking, there are two devices that can be used to pay with the digital euro as displayed in figure 7: a mobile device or a smart card (ECB, 2024b, p. 6). A smart card is a physical card with a battery that omits the bridge device and provides the ECB more control over the secure element (ECB, 2024d, p. 9).

Mobile devices and smart cards carry different cyber privacy risks. Mobile devices contain more information than cards, but also better secured, since mobile devices are capable of using biometric data for payment authentication, where card payments only require an uncomplicated PIN. The risk of using biometric identifiers is that the data cannot be changed in case it is leaked to a malicious actor (BIS, 2023, p. 50). Furthermore, mobile devices uses more communication technologies that opens up the risks of phishing or disruption through various communication channels. For example, the ECB experimented with Bluetooth, only applicable to electronic devices (ECB, 2021b, p. 7).

Both mobile devices and (smart) cards can make contact through near-field communication (NFC), which is a communication technology already apparent in most mobile devices and cards. NFC builds on the secure element within devices, which is a "microprocessor chip that protects sensitive data by providing tamper-resistant storage and processing of cryptographic keys and other security-critical information" (ECB, 2024b, p. 5). The ECB wants to use this secure element to be able to store keys and handle digital euro transactions. Compromising a device with a secure element is difficult without manufacturers' help (Christodorescu, 2020, p. 4). This makes secure elements a viable option for the digital euro, but also an inflexible one, since the Eurosystem doesn't produce its own secure element. Even though most regular cards have NFC functionality, non-powered cards can't make payer-initiated payments, in contrast to mobile devices or smart cards. Rather, the other device would initiate a payment and the card can accept the payment through proximity contact. Regular cards lack a secure element, which makes it impossible to store information and enforce holding limits, rendering cards a relatively unviable option for offline payments. Also, dependence on payee-initiated payments carries more risk, since some trust or vigilance is needed by the payer. But still, the ECB has been investigating a "bridge device" that can connect two non-powered cards, which

is a “simple, pocket-sized, battery-powered device for establishing a connection” (ECB, 2023b, p. 5). This bridge would enable P2P payments.

The offline use case risks predominantly play out in the proximity of the device. Both mobile devices and smart cards are susceptible to NFC attacks like skimming, which triggers an unintended transaction. Furthermore, it is possible to secretly eavesdrop information during a NFC interaction, committing a man-in-the-middle attack (Kortvedt & Mjolsnes, 2009, p. 58). Lastly, since data is stored on the secure element of the local storage device, funds will be lost when the device is stolen (ECB, 2023d, 14).

Online use case

In the ECB reports, there is no clear depiction of the form factors of the online digital euro. The use cases of the online digital euro are online P2P payments and e-commerce payments. It is unclear if offline payments could be made despite have connection to the Internet (CEPS, 2023, p. 22). The proximity risks of the offline digital euro carry over to the proximity risks of the online digital euro (e.g. NFC risks). But because the online digital euro offers less privacy, funds will be kept on the account in case of device theft. On the other hand, the connection to the Internet opens up an array of extra risks. For example, the ECB plans to use QR codes to identify users or to initiate transactions (ECB, 2024c, p. 17). A malicious actor could attempt phishing with an altered QR.

In terms of e-commerce, the amount of vulnerabilities provide an increase in cyber privacy risks. Phishing attempts, and other forms of social engineering, are more prevalent on the Internet, due to a variety communication technologies. Furthermore, in case of the online digital euro, criminals are not limited to proximity crimes.

5.2.2. Account-based versus token-based and centralized versus decentralized

This section revolves around the technology and involved architecture that is needed for the digital euro to operate. At the time of the first report in 2020, it is unclear if the digital euro will be account based or token-based. The ECB states that the digital euro may be provided either through an account-based system or as a bearer instrument (ECB, 2020, p. 29) even speculating at a coexistence (ECB, 2020, p. 35). Privacy is high on the agenda, so the ECB chooses the option that provides the highest privacy, taken into account its feasibility. Since, account-based requires a ledger that verifies identity, token-based should be the more private

option. However, the online digital euro is token-based and the offline implementation of the digital euro is account-based. In terms of architecture technology, the impact assessment (ECB, 2023b, p. 10) states that the digital euro is technology-neutral, meaning that they left the options open for alternative technologies, such as DLT. As of now, it looks like the online digital euro will be centralized, while the offline digital euro will have elements of both centralized and decentralized.

Online

In this digitized world, where the majority of payments are made remotely and the prevalence of e-commerce is increasing, the digital euro should also be able to facilitate this feature. Furthermore, implementing both online and offline modes to ensure most coverage of usage and prevents reliance on either an internet connection or a bearer instrument (ECB, 2023d, p. 13). Since the online digital euro is token-based and doesn't rely on accounts with balances, another way of validating payments is needed to avoid the double spending problem. Even though token-based CBDCs are often associated with a decentralized structure, the digital euro will have a centralized ledger for validation. However, DLT technology has inspired the digital euro to adopt one of its core technologies. The online prototype activities experimented with a centralized settlement developed by the Eurosystem, called N€XT, that is based on a Unspent Transaction Output (UTXO) data model (ECB, 2023b). The UTXO model is used with Bitcoin (Delgado-Segura et al., 2019, p. 78). A UTXO is a token that has a specific value, so there is no balance portraying a total amount of money. Instead, a wallet contains UTXOs with fixed values. UTXO is comparable to cash in the sense that a physical wallet with cash consists of several different banknotes and coins. The payer chooses the combination of how to spend those physical tokens, instead of a balance reduction on the account. If a holder wants to spend its UTXO, a private key as proof is needed to sign the payment transaction (Chan, 2021, p. 10). The holder's identification isn't necessary, since the private key is enough proof of ownership of the token. Just like tearing a banknote is not the smartest idea, a UTXO cannot be partially spent to pay an amount lower than the token. Rather, two new UTXOs are created, with one going to the payee as a payment, while the other returns to the payer as change (Chan, 2021, p. 10). It is unclear how this technology will be portrayed in the front-end user interfaces.

In the Bitcoin white paper, there is no mention of wallets, but Nakamoto (2008, p. 3) refers to addresses as public keys. So there is a private key that is used by an owner to spend a UTXO and there is a public key that others can use as an address to make a transaction to. The public

keys or addresses of end users in the Eurosystem are referred to the digital euro account number (DEAN).

A feature that UTXOs have, which account-based models can't have since the system needs to verify the identity and balance of the account holder, is the hashing of transactions. Both public and private keys are hashed, which is a technique that creates a certain output based on the input. Irrespective of the length of the input, hashing results in a cryptographic output with a fixed value, which should be a one-way function, meaning that the output should be irreversible to the input (Chi & Zhu, 2017, p. 5). This output is called a hash, and the same input always creates the same hash. For example, the digital euro will use a strong hash to pseudonymize user identifiers, the public keys (ECB, 2024a, p. 4). Users' credentials in a Eurosystem database are hashed and instead of the credentials, the hash itself is stored in the database. When a user logs in to the digital euro app, the user's input is the regular password. This password is the hashed and since the same inputs create the same hashes, if the password is correct the hash should correspond with the hash stored in the database. Hashing is different from encryption, because hashing is an irreversible one-way function, where encryption is a two-way function that requires a key to decrypt the data. The benefit of hashing is the fact that the PSP doesn't need to know the user's credentials at any point of time. However, since hashing is a form of pseudonymization and the hash is theoretically, yet almost unfeasibly, possible to decrypt, the data is not anonymous and falls under GDPR.

This UTXO model creates a token system where identity is irrelevant and a third party is not required to validate that the payer does indeed have money. However, the UTXO model in itself doesn't solve the double spending problem. Hence, a ledger is still needed to record all transactions. This ledger, the N€XT settlement engine, is the back-end's central building block. Early in the development process, both traditional technology or alternative technologies such as DLT were still options, but it transpired that a third party would be involved (European Commission, 2023b, p. 10). Since the digital euro is aimed at the large consumer market and decentralization suffers scalability, centralization enables a scalable engine that ensures low latency of transaction processing (ECB, 2023b, p. 5). Not only does the ECB estimate that the UTXO format on a centralized ledger is future proof, because it supports many types of transactions and can be extended, it should also enable high privacy. As mentioned, the UTXO model itself requires no identification, since the ledger only verifies one-time UTXO addresses (ECB, 2023b, p. 8). In order to process the UTXO transaction, the

ledger has no information on the wallet, identity or even pseudonym of the owner. In the N€XT settlement engine, there are two ledgers: a transaction ledger and a UTXO ledger. The UTXO ledger is needed for the functioning of the model and destroys spent UTXOs. The transaction ledger provides a historical record of all transactions. The benefit of such a ledger is that transactions can be reversed with the help of an intermediary, for example when the wrong DEAN is used. Theoretically, this system protects the data of end users, but this data protection isn't endless, since there are AML/CFT checks and possible holding limits, which will be discussed later.

Offline

An offline digital euro operates without an internet connection. This could be useful in cases where there is weak or even no internet connection available, for example due to a lack of network infrastructure or due to power outages. The lack of an internet connection has implications. First, the ways of contact between payer and payee are limited to proximity payments, since a form of direct contact is required. Second, where the online model builds on the constant existence of the ledger, the offline model operates in absence of this ledger, since the ledger is dependent on connection to the internet. This means that the UTXO model, which requires a ledger to record transactions, isn't suitable for the offline digital euro. Also, it would seem that an account-based system is off the table, since transactions require real-time verification against an account balance held on a central ledger.

However, completely against the author's expectations, the offline digital euro is in fact account-based with a centralized ledger. At least, this statement is based on what is known so far, since the offline digital euro is still under development. The only mention of the offline digital euro being account-based is in ECB's report about the offline prototype, calling the offline prototype data model "balance-based, as opposed to the UTXO-based data model for the online back-end prototype" (ECB, 2023b, p. 12). During transactions, there is no way to make contact to the ledger, but instead the transactions are kept within the two parties involved through secure hardware. The secure element keeps the balance and this chip allows to make decentralized transactions where no third party is needed. Account-based and balance-based both are characterized by the fact that the account balance is stored on a ledger, often at a commercial bank. The balance of this offline digital euro is stored on the ledger of the local storage device, which implies higher privacy than on an external ledger. However, this is under the condition that the device is prefunded. However, funding or defunding the

device would need to be managed online (ECB, 2020, p. 34). This is because the local storage device has to be identified, due to holding limits and AML, and the system checks if the defunded digital euro is genuine to prevent the double spending problem and forgery (ECB, 2024d, p. 13). This makes the offline digital euro is centralized, but since the balance is stored on the local ledger, the centralized aspect revolves around the control of the money supply. In summary, the transactions made with an offline digital euro are decentralized and quite private, while the funding and storage of the digital euro is centralized and less private. Like the online digital euro, the offline digital euro has the potential to become a very private currency. However, the offline model again has limits in privacy to ensure that there are AML/CFT checks during the funding and defunding processes (ECB, 2023b, p. 6). It would be technically feasible to develop a digital euro without the need for online funding, but creating a currency with full anonymity was never the ECB's intention (ECB, 2022b, p. 7).

5.2.3. Direct versus indirect

The design choice between direct and indirect was also quite predictable and consistent from the beginning. One of the goals of the digital euro is providing digital central bank money to the public. Since commercial bank deposits is private money, which carries more risks, the ECB has repeatedly stated that the digital euro will be central bank money. This means that the digital euro will either be direct or hybrid. Since direct is unfeasible, due to the amount of accounts and the lack of experience, and for the most part there is an existing payment infrastructure that can support the digital euro, the digital euro will be hybrid. The ECB would be a supervisory authority over the PSPs and holders of the digital euro would have a direct claim on the ECB or their national central bank. The PSPs have a range of intermediary tasks similar to the commercial banking system, consisting of access management, transaction management and liquidity management (ECB, 2024c, p. 5). Also, PSPs are responsible for performing AML checks at different stages.

Intermediary tasks

First, the PSPs are responsible for access management. During the onboarding, KYC checks are performed according to existing laws and regulations and the end users are provided with digital euro services (ECB, 2023d, p. 12). Among these services are creating an account and a DEAN which can be accessed through the app. End users also receive a payment instrument when needed. Onboarding is provided either remote or physical to maximize financial

inclusion (ECB, 2024c, p. 6). In case the end user is known to the PSP, which is likely since 98,5% of euro area citizens have an account at a financial institution, that available data will be reused for the onboarding of the digital euro (ECB, 2022c, p. 8). PSPs are also in charge of the offboarding process. Even though the financial inclusion is maximized through inclusive onboarding, the onboarding still follows existing regulations, just like commercial banks. This implies that the KYC checks are evenly strong in the two cases and therefore is the digital euro onboarding not more inclusive. Furthermore, the digital euro onboarding handle the same data and is not more private than an onboarding at a commercial bank. The inclusivity lies in the fact that consumers can open a digital euro bank account at another PSP than a commercial bank.

Second, the PSPs manage the processing of digital transactions, including authentication, payment initiation and payment confirmation (ECB, 2024c, p. 5). Akin to the commercial banking system, PSPs perform AML checks during transactions. During transactions of private money and central bank money, commercial banks and digital euro PSPs process only the information that is necessary for the transactions. As established, an account-based system verifies both parties and validates their balances in order to transact the payment. The online digital euro's UTXO model doesn't require an identification during a payment, rather the hashed private key that is than hold against the hash in the centralized Eurosystem ledger. The transaction is more secure in the case of the online digital euro, since data is hashed when criminals manage to intercept it, in contrast to commercial bank transaction. What's more, the offline digital euro's transactions are not traced outside of the local storage ledgers.

Third, liquidity management is about managing the amount of digital euro in circulation, including the funding and defunding of accounts (ECB, 2024c, p.5). In other words, PSPs manage the holdings of end users and the amount of these holdings. The ECB aims to minimize the impact of the digital euro on the financial system, endangering the role of commercial banks (ECB, 2023f, p. 4). To facilitate this, holdings limits are enforced. These holding limits are yet to be determined, but have a lot of implications on the digital euro liquidity management. For example, in terms of funding and in case of multiple accounts per DEAN.

Funding

Funding and defunding is essentially a reallocation of a euro to another form and could be done with cash or commercial bank deposits. With both the online and offline digital euro, funding always happens online. Transferring money from a commercial bank account to an offline digital euro account is essentially the same as getting cash from an ATM. In fact, there will be designated ATMs for the funding of the offline digital euro (ECB, 2024b, p. 4). However, the holding limits complicate things a lot. The funding and defunding processes provide the PSP with information on the end user and make end users vulnerable to various cyberattacks at an ATM (e.g. phishing, eavesdropping). Holdings limits increase the amount of information by increasing necessary actions. Furthermore, holdings limits are highly unpractical. Depending on the height of the limit of course, the digital euro account needs to be funded more often than without limits. This increases moments of information disclosure, especially for the offline digital euro, and decreases user friendliness. The ECB has thought of a service to solve this impracticality: the waterfall functionality. The waterfall functionality allows users to receive payments in digital euro above the holding limit by linking a commercial bank account (ECB, 2024c, p. 15). This mechanism, exclusively for the online digital euro, enables users to redirect the received funds that exceed the holding limit to their private account. This is alike automated defunding. Furthermore, the waterfall functionality allows users to set a lower holding cap than the Eurosystem limit (ECB, 2024c, p. 17). . A similar solution is presented, called reserve waterfall functionality, in cases where the user is making a payment, but the digital euro holdings are lower than the transaction value (ECB, 2024c, p. 15). This way purchases with a transaction value higher than the user's holdings could be funded automatically through the chosen commercial bank account. The reverse waterfall is a form of automated funding. The offline digital euro is not compatible with the (reverse) waterfall functionality, but does have holdings limits. In fact, the ECB hints at lower holding limits for the offline digital euro to lower the risk of criminal misuse (ECB, 2023d, p. 38). Even though the waterfall functionality increases payment efficiency, it is another source for cyber privacy risks. The holding limits could protect end users in cases of theft, since there is a maximum that could be stolen directly. The linkage between commercial bank accounts and digital euro accounts increases this maximum by a great amount. Furthermore, the linkage provides the PSP with more personal data but this amount isn't necessarily increased due to the waterfall functionality, since the commercial bank account was likely to be known already due to funding processes. Still, this linkage could increase the value of data theft.

For merchants, there is zero holding limits, which means that transactions are made and received with digital euro, but they aren't allowed to hold any (ECB, 2023d, p. 12). In order to make payments without holdings, implementing the waterfall functionality is compulsory for merchants. This is again to minimize impact on the financial system. It would also enable merchants to have an unlimited number of digital euro accounts, that could be useful to split branches (ECB, 2022c, p.11).

Account management

In contrast to merchants, end users are not able to have unlimited accounts, but they are allowed to have multiple. Even though the management of several accounts per end user is technically feasible, it is a trade off in terms of user experience (ECB, 2024a, p. 5). For the most part this is due to the fact that holding limits are not linked to the account, but to the DEAN. This means that an end user's holding limits don't increase with multiple accounts and that the end user is responsible for managing the holdings limits across the accounts. There are a few complications here that worsen user experience. First, the end user has to reallocate the holding limits of current accounts when opening a new one (ECB, 2024a, p. 7). In case there is no waterfall functionality or an offline account, the account potentially needs to be defunded first. The end user also has to decide how to split the holding limits across the different accounts. Second, the ECB introduces the "switch-and-port" functionality, which lets users easily change PSP while maintaining their DEAN (ECB, 2024a, p. 2). Users are free to switch, which might come in handy in case of "exceptional circumstances" where a PSP is operationally uncapable (European Commission, 2023a, Art. 31). This functionality doesn't just let users switch accounts, the accounts can also coexist. In contrast to IBAN, the DEAN doesn't embed a country code and PSP code, which enables the identifier to be ported (ECB, 2024a, p. 2). This complicates the holding limits, since they can be spread out over multiple accounts at multiple PSPs, which requires both sharp management and communication. According to the PSD2, not only bank entities can become a PSP, diversifying the options for end users (European Parliament and Council of the European Union, 2015). The Eurosystem will develop a digital euro app for these new PSPs that often have no bank app (ECB, 2023b, p .13). To decrease the risk of disposing personal data due to a variety of PSP actors, contact between end users and PSPs and between PSPs will be encrypted (ECB, 2024b, p. 3).
In order to minimize the data of this variety of accounts, a single access point (SAP) is proposed, which is a repository for DEANs and other related data, accessible for all PSPs (ECB, 2024a, p. 3). This allows all PSPs to easily check the pseudonymized database without

the need to transfer data between PSPs. The SAP would be proposed irrespective of the multi account scenario, since the SAP allows PSPs to enforce holding limits and emergency PSP switching. Even though the existence of a centralized database accessible to all PSPs fosters efficient functioning, it bears the risk of being a single point of failure. On the one hand, once cybercriminals have access to the SAP, they have access to all data. Since the data on the SAP is hashed, this significantly lowers the risk. On the other hand, however, through a successful DDoS attack the whole database could be disrupted, compromising CIA. The joint opinion (EDPB-EDPS, 2023, p. 16) underscores the option for decentralized storage of this data, as an alternative.

6. Discussion

In this section, the major findings of the previous chapter are discussed. The potential implementation of the digital euro will be placed in the context of the current retail landscape of the EU and compared to cash and commercial bank deposits. As the ECB (2024e) states, the digital euro won't be as private as cash, but close. The comparison between cash and the digital euro, especially the offline variant, is based on the fact that the two forms of money share high anonymity. Another similarity between cash and the offline digital euro is its use case. The digital euro has different use cases across the online and offline implementation. Cash and the offline digital euro can both be used in proximity P2P (and POS) payments, but not in payments that require an internet connection, such as remote payments and e-commerce. This resemblance enables a valid comparison in terms of cyber privacy risks. Likewise, both commercial bank deposits and the online variant of the digital euro handle not only proximity payments, but also remote payments. These forms of money are comparable in its broad coverage of use cases and provide another valid comparison.

6.1. Comparison between the offline digital euro and cash

Cash and the online digital euro are too different to make a valid comparison. For example, cash inherently carries no cybersecurity risks and no technical vulnerabilities. Cash isn't susceptible to phishing, DDoS or malware, because cash is no part of cyberspace. This also means that the benefits of a digital currency, such as remote payments and an account, don't apply to cash. Since cash doesn't contain information, there are no cyber privacy risks in

itself. So while cash is definitely more private than the digital euro, especially the online variant, the purposes and use cases are very different. The offline digital euro on the other hand share more similarities to cash. The offline digital euro is the more private half of the digital euro and is bounded by proximity payments, just like cash.

Even though "cash-like" CBDC typically refers to token-based CBDC, the digital euro is technically account-based and especially resembles cash in terms of funding and transactions. The offline digital euro requires an internet connection to fund or defund the balance on the local storage device. Withdrawing cash from an ATM uses a commercial bank account and also requires an internet connection. However, cash could be handed over from another person without leaving any sort of data trail, which a digital euro cannot do. This means that the risks of online funding and withdrawing from an ATM don't apply to cash. It is unclear how risky the designated digital euro ATMs will be, but expectedly there will be the usual proximity risks (e.g. skimming, eavesdropping).

In terms of transactions, the balance-based offline euro manages transactions with a privacy close to cash in a decentralized way. Both forms of money are limited to proximity payments. The Eurosystem knows the amount of money on the local storage device in intervals, since the funding and defunding provides the Eurosystem with an update. This is also due to the holdings limits that are being enforced. The Eurosystem doesn't know where the money is going to in between funding and defunding. The benefit of the offline digital euro compared to cash is that the payment can be made digitally, fostering financial inclusion in places where cash payments are no option. However, since cash doesn't leave a data trail in transactions and storage, it is not susceptible for any cyberattack. Even though the secure element in mobile phones offer great security to the end user, if criminals find a way to break the secure element, phones will become an even more attractive target for theft, resulting in a loss higher than just funds.

In this point of time, it is not possible to judge the security of the bridge device or smart card, since they are still in development. However, the usage of any device brings data to the table and opens up the possibility of data theft. The fact that cash is a real physical token, without dependence on anything but itself, eliminate privacy risks to nearly zero.

In terms of privacy, cash will always be the better option. While the movement of cash will never contain any form of data, offline usage of anything, with theoretically perfect privacy and data protection, will still be electronic and therefore inherently leaves a data trail, albeit

secured. There is a reason why cash is appreciated by criminal for its anonymous qualities (Riccardi & Levi, 2018, p. 53).

6.2. Comparison between the digital euro and commercial bank money

Where cash and the digital euro doesn't provide a fair comparison, commercial bank money is a lot more similar. Both these forms of money are capable of P2P payments and e-commerce, but the digital euro has a broader coverage of online and offline use cases.

Online digital euro and commercial bank money are indirect in its use of intermediaries. The digital euro is actually hybrid since the digital euro is liability of the central bank, but in terms of functioning the two types of money are close. Both use PSPs that handle the onboarding and offboarding of end users and in both cases PSPs are responsible for AML/CFT. Since the regulations regarding the GDPR and AMLD6 apply as much to the digital euro as to the commercial bank context, the amount of personal data that is collected should be the same. The PSP landscape of the digital euro is more fluid than with commercial bank money, since changing digital euro PSPs will be possible without too much effort. The rigidity of the commercial bank system is not only because of the embedded country and bank in the IBAN, but also due to the difference in what commercial and central banks are trying to achieve. Both want to keep as many clients as possible, but the central bank is not limited to one PSP, while a commercial bank inherently is. In case of the digital euro, there might even be multiple PSPs per user. According to the ECB, this does not increase cyber privacy risks, since there is a single access point which PSP utilize to identify users and such. However, even if there is a single access point, the end users personal data is still connected to multiple PSPs, creating a greater attack surface. For example, in the case that a user has accounts at multiple PSP, the users has probably also several banking apps, again creating a bigger attack surface. There will be a secure digital euro app, but in case a criminals forces his way in, it might be repeatable, carrying a greater total risk than one PSP. The choice of having multiple at various PSP is that of the end user. The risk of uniformity also applies to the single access point. Once the single access point is breached, large amounts of data could be compromised. The single access point is hashed, but since hashing could theoretically be cracked, there is still a risk (Tatli, 2015). The role of the intermediaries diminishes the potential of the digital euro in terms cyber privacy risks. Both AML and the enforcement of holdings limits impose a lot of PSP monitoring and a greater attack surface for cybercriminals.

In terms of form factors, the online digital euro and the commercial banking system both use the Internet, which opens up all kinds of social engineering risks. Phishing is a growing threat to e-commerce (Banday & Qadri, 2011). There is no reason to assume that the digital euro is more resistant to social engineering than commercial bank money, since that responsibility lies mostly in the hands of the end user. Also, it is not yet clear how secure the form factors of the digital euro will be.

Perhaps the most important distinction in terms of cyber privacy risks is that the online digital euro is token-based and commercial bank money is account-based. The fact that the online digital euro is token-based enables certain encryption measures in which hashing plays a pivotal role. During transactions, instead of a verification of identity and balance, a hashed private key is used as authentication of ownership. The DEANs of the payer and potential payee are also hashed. This means that in case of a criminal data breach, less personal data is exposed, since online digital euro transactions contain less information than commercial bank money transactions. The two hashed ledger of the online digital settlement hold less personal information than a commercial bank ledger. Furthermore, the digital euro ledger is the only ledger that is required for a digital euro payment. In the current commercial banking system, commercial bank ledgers are not directly connected to each other, which means that transactions involving two banks must be routed through the central bank's ledger (CEPS, 2023, p. 6). Both the digital euro and commercial bank ledger are centralized, which are single point of failure and are susceptible to DDoS attacks.

The asset that makes the digital euro more private and secure is the compatibility with both online and offline. The online digital euro is likely to be more private than commercial bank money in e-commerce and P2P use cases, but the digital euro can also be used offline in cases of proximity payments. This flexible option favors the digital euro to commercial bank money.

6.3. Limitations of the research

This research acknowledges several limitations. Firstly, the digital euro has not yet been implemented, making the analysis somewhat speculative, as noted by Xu (2022, p. 238), who describes researching CBDCs as "like researching a ghost." Unforeseen risks, or unknown unknowns, may only become apparent once the digital euro is operational, and there remains a possibility that the digital euro may not be issued at all.

Secondly, while the ECB and EU are relatively transparent, the research is dependent on publicly disclosed information. It is unlikely that all considerations, especially those pertaining to cybersecurity risks, are made public by the ECB, whose publications primarily aim to inform end users about potential future currency development. The publications are also biased, since the ECB wants to convince the public of the digital euro's relevance.

Third, this research is highly interdisciplinary, which draws on fields such as law, finance, cybersecurity, and privacy. Therefore, with absolute certainty, this research contains oversimplifications or the overlooking of certain nuances. Likewise, this risk assessment is not exhaustive by any means, which leaves room for further investigation, once the ECB has published more reports.

7. Conclusion

This thesis investigated the cyber privacy risks of the digital euro that might be issued by the ECB in a few years. Both the online and offline implementations are discussed and compared to existing forms of money: cash and commercial bank money. The analysis was grounded in the four dichotomies by Bossu et al. (2020) that were applied to both the online and offline digital euro. The research question that this thesis aimed to answer was: *"How do the cyber privacy risks for end users of the digital euro in both its online and offline implementations compare to existing forms of money, such as cash and commercial bank money?"* The conducted research provides a few conclusions.

First, based on the ECB publication it seems like that both of the implementations of the digital euro will indeed be both quite private and secure. Cash will always win in terms of privacy, but is very limited in its use. For a digitized option, the digital euro is viable. Especially the UTXO model paves the way for a private and secure landscape, due to hashing and its token-based character. Also, PSP will have access to less information in the digital euro system. When the amount of personal data is minimization, the impact of a successful data breach is also lower. However, there are some limits to this conclusion. First, the effectiveness of digital euro is diminished by AML and holding limits, but financial institutions need to enforce AML and perhaps the holding limits will change over time. Second, the ECB has developed various prototypes of certain parts of the digital euro

settlement, but is still dependent on other manufacturers that develop technologies, such as NFC and secure elements. This means that the ECB hasn't full control over the technologies and need to cater their inventions. Third, while the digital euro is indeed more private and secure than commercial bank money, the digital euro is explicitly no replacement for any form of money. Instead, the digital euro is complementary and often makes use of the commercial bank accounts especially due to the holding limits. Thus, the digital euro actually increases the attack surface for criminals. Lastly, since the digital euro will need a few more years of development, a lot can change. Not only will cybercriminals use new methods to exploit vulnerabilities, there will always be unknown unknowns, especially in new developments.

Second, while the digital euro uses state-of-the-art technologies, the focus of the ECB publications is predominantly on the technical side of cyberspace and not so much on the socio-technical side. As portrayed by Van den Berg et al. (2015) cyberspace consists of three layers and to board up the whole of cyberspace, all three layers need to be considered. Since humans are the weakest link, this layer needs at least the same amount of attention. Social engineering is boosted by the advent of ChatGPT, deepfakes and other forms of AI, which enables an increase in possibilities for cybercriminals. Furthermore, the world is still getting more interconnected and the exposure to cybercriminals worldwide keeps increasing accordingly. Likewise, due to AI both cyber-dependent and cyber-enabled crimes will garner more success.

The good news is that major European financial institutions join forces against cyberthreats (ECB, 2024f). The digital euro has the potential to provide the residents at the euro area with a private and secure payment method, because of the successfully experimentation by the ECB with a variety of technical prototypes. Now, it is time to tackle the human vulnerabilities.

8. Literature

Adam, B., & Van Loon, J. (2000). Introduction: Repositioning risk; the challenge for social theory. *The risk society and beyond: Critical issues for social theory*, 1-31.

Agur, I., Ari, A., & Dell'Ariccia, G. (2022). Designing central bank digital currencies. *Journal of Monetary Economics*, *125*, 62-79.

Ahnert, T., Hoffmann, P., & Monnet, C. (2022). The digital economy, privacy, and CBDC.

Aiello, S. (2024). Privacy Principles and Harms: Balancing Protection and Innovation. *Journal of Cybersecurity Education, Research and Practice*, *2024*(1), 1-9.

Ambore, S., Richardson, C., Dogan, H., Apeh, E., & Osselton, D. (2017). A resilient cybersecurity framework for Mobile Financial Services (MFS). *Journal of Cyber Security Technology*, *1*(3-4), 202-224.

Amoo, O. O., Atadoga, A., Osasona, F., Abrahams, T. O., Ayinla, B. S., & Farayola, O. A. (2024). GDPR's impact on cybersecurity: A review focusing on USA and European practices. *International Journal of Science and Research Archive*, *11*(1), 1338-1347.

Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2020). Operational and cyber risks in the financial sector. *International Journal of Central Banking*, 19(5), 341-402.

Appendino, M., Bespalova, O., Bhattacharya, R., Clevy, J., Geng, N., Komatsuzaki, T., Lesniak, J., Lian, W., Marcelino, S., Villafuerte, M., Yakhshilikov, Y. (2023). Crypto assets and CBDCs in Latin America and the Caribbean: opportunities and risks. IMF Working Papers, no 37, February.

Arfelt, E., Basin, D., & Debois, S. (2019). Monitoring the GDPR. In *Computer Security–ESORICS 2019: 24th European Symposium on Research in Computer Security, Luxembourg, September 23–27, 2019, Proceedings, Part I 24* (pp. 681-699). Springer International Publishing.

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

Assante, M. J., & Lee, R. M. (2015). The industrial control system cyber kill chain. *SANS Institute InfoSec Reading Room*, *1*(1), 2.

Atlantic Council. (n.d.). *Central bank digital currency (CBDC) tracker*. Atlantic Council. https://www.atlanticcouncil.org/cbdctracker/

Bambauer, D. E. (2013). Privacy versus security. *J. Crim. L. & Criminology*, *103*, 667.

Banday, M. T., & Qadri, J. A. (2011). Phishing-A growing threat to e-commerce. *arXiv preprint arXiv:1112.5732*.

Banisar, D. & Davies, S. (1999). 'Global trends in privacy protection: an international survey of privacy, data protection and surveillance laws and developments', J. Marshall J. Computer & Info. L. 1999, Vol. 18, no. 1.

Bank for International Settlements. (2017). Central bank cryptocurrencies. *BIS Quarterly Review September*.

Bank for International Settlements. (2018). Central bank digital currencies, BIS Committee on Payments and Market Infrastructures, Market Committee, March.

Bank for International Settlements. (2019a). Wholesale digital tokens.

Bank for International Settlements. (2019b). Proceeding with caution-a survey on central bank digital currency.

Bank for International Settlements. (2020a). Rise of the central bank digital currencies: drivers, approaches and technologies.

Bank for International Settlements. (2020b). *Covid-19, cash, and the future of payments* (No. 3). Bank for International Settlements.

Bank for International Settlements. (2020c). The technology of retail central bank digital currency. *BIS Quarterly Review, March*.

Bank for International Settlements. (2021). *Central bank digital currency: the quest for minimally invasive technology* (No. 948).

Bank for International Settlements. (2023). Central bank digital currency (CBDC) information security and operational risks to central banks.

Bank for International Settlements. (2024) Embracing diversity, advancing together - results of the 2023 BIS survey on central bank digital currencies and crypto.

Bank of England. (2015). *One Bank Research Agenda.*

Beck, U. (1992). *Risk society: Towards a new modernity* (Vol. 17). sage.

Bhatia, N. L., Shukla, V. K., Punhani, R., & Dubey, S. K. (2021, June). Growing aspects of cyber security in e-commerce. In *2021 International Conference on Communication information and Computing Technology (ICCICT)* (pp. 1-6). IEEE.

Bibi, S., & Canelli, R. (2023). The interpretation of CBDC within an endogenous money framework. *Research in International Business and Finance*, *65*, 101970.

Bindseil, U. (2019). Central bank digital currency: Financial system implications and control. *International Journal of Political Economy*, *48*(4), 303-335.

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance-Issues and Practice*, *40*, 131-158.

BIS Innovation Hub (2023a). Project Polaris: a handbook for offline payments with CBDC, May. https://www.bis.org/publ/othp64.htm

BIS Innovation Hub (2023b). *Project Polaris: high-level design guide for offline payments*. https://www.bis.org/publ/othp79.htm

Bofinger, P., & Haas, T. (2020). CBDC: Can central banks succeed in the marketplace for digital monies?.

Boeckl, K., Boeckl, K., Fagan, M., Fisher, W., Lefkovitz, N., Megas, K. N., Nadeau, E., O'Rourke, D.G., Piccareta, B. & Scarfone, K. (2019). *Considerations for managing Internet of Things (IoT) cybersecurity and privacy risks*. U.S. Department of Commerce, National Institute of Standards and Technology. Gaithersburg, MD.

Bolt, W., Lubbersen, V., & Wierts, P. (2022). Getting the balance right: crypto, stablecoin and CBDC.

Bossu, W., Itatani, M., Margulis, C., Rossi, A., Weenink, H., & Yoshinaga, A. (2020). Legal aspects of central bank digital currency: Central bank and monetary law considerations. Bouchaud, M. *et al.* (2020) *Central banks and the future of digital money*. doi: 10.2139/ssrn.3369649.

Bouveret, A. (2018). *Cyber risk for the financial sector: A framework for quantitative assessment*. International Monetary Fund.

Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press, USA.

Broadbent, B. (2016). Central banks and digital currencies.

Bygrave, L. A. (2010). Privacy and data protection in an international perspective. *Scandinavian studies in law*, *56*(8), 165-200.

Cambridge University Press. (n.d.). *Risk*. In *Cambridge Dictionary*. Retrieved from https://dictionary.cambridge.org/dictionary/english/risk

Carr, M. (2016). Public–private partnerships in national cyber-security strategies. International Affairs, 92(1), 43–62.

Cavelty, M. (2013). From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review*, *15*(1), 105-122.

Cebula, J. J., & Young, L. R. (2010). A taxonomy of operational cyber security risks. *Software Engineering Institute, Carnegie Mellon University*.

Centre for European Policy Studies. (2023). *A digital euro: Beyond impulse, think twice, act once*. https://cdn.ceps.eu/wp-content/uploads/2023/10/A-digital-euro-beyond-impulse-think-twice-act-once.pdf

Chan, A. C. (2021). UTXO in Digital Currencies: Account-based or Token-based? Or Both?. *arXiv preprint arXiv:2109.09294*.

Cheng, L., Liu, F., & Yao, D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *7*(5), e1211.

Collier, G. (1995). Information privacy. *Information Management & Computer Security*, *3*(1), 41-45.

Conteh, N. Y., & Schmick, P. J. (2021). Cybersecurity risks, vulnerabilities, and countermeasures to prevent social engineering attacks. In *Ethical hacking techniques and countermeasures for cybercrime prevention*, 19-31.

Cœuré, B. (2018, November 15). *The new frontier of payments and market infrastructure: on cryptos, cyber and CCPs* [Speech]. European Central Bank. https://www.ecb.europa.eu/press/key/date/2018/html/ecb.sp181115.en.html

Chi, L., & Zhu, X. (2017). Hashing techniques: A survey and taxonomy. *ACM Computing Surveys (Csur), 50*(1), 1-36.

Chung, W., & Paynter, J. (2002). Privacy issues on the Internet. In *Proceedings of the 35th Annual Hawaii International Conference on System Sciences*, 1-9.

Davoodalhosseini, S. M. (2022). Central bank digital currency and monetary policy. *Journal of Economic Dynamics and Control, 142*, 104150.

Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Frontiers in psychology, 9*, 744.

de Dios, M. A. (2015). The sixth pillar of anti-money laundering compliance: Balancing effective enforcement with financial privacy. *Brook. J. Corp. Fin. & Com. L., 10*, 495.

De Hert, P., & Gutwirth, S. (2009). Data protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in action. In *Reinventing data protection?* (pp. 3-44). Dordrecht: Springer Netherlands.

Delgado-Segura, S., Pérez-Sola, C., Navarro-Arribas, G., & Herrera-Joancomartí, J. (2019). Analysis of the bitcoin utxo set. In *Financial Cryptography and Data Security: FC 2018 International Workshops, BITCOIN, VOTING, and WTSC, Nieuwpoort, Curaçao, March 2, 2018, Revised Selected Papers 22* (pp. 78-91). Springer Berlin Heidelberg.

Dwyer, G. P. (2015). *The economics of Bitcoin and similar private digital currencies.* Journal of Financial Stability, 17, 81-91.

European Data Protection Board & European Data Protection Supervisor. (2023). *EDPB-EDPS Joint Opinion 02/2023 on the Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro*. https://www.edpb.europa.eu/system/files/2023-10/edpb_edps_jointopinion_022023_digitaleuro_en.pdf

European Central Bank. (2018, November 15). *The new frontier of payments and market infrastructure: on cryptos, cyber and CCPs* [Speech]. European Central Bank. https://www.ecb.europa.eu/press/key/date/2018/html/ecb.sp181115.en.html

European Central Bank. (2020a, October 2). *Report on a digital euro. https://www.ecb.europa.eu/euro/html/digitaleuro-report.en.html*

European Central Bank. (2020b, October 2). *ECB launches public consultation on a digital euro*. https://www.ecb.europa.eu/press/pr/date/2020/html/ecb.pr201002~f90bfc94a8.en.html

European Central Bank. (2021a, July 14). *Eurosystem launches digital euro project*. https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210714~d99198ea23.en.html

European Central Bank. (2021b). *Digital euro experimentation scope and key learnings* (Publication No. 2021/07). https://www.ecb.europa.eu/pub/pdf/other/ecb.digitaleuroscopekeylearnings202107~564d89045e.en.pdf

European Central Bank. (2022a). *Study on the payment attitudes of consumers in the euro area (SPACE): 2022 report*. https://www.ecb.europa.eu/stats/ecb_surveys/space/html/ecb.spacereport202212~783ffdf46e.en.html#toc7

European Central Bank. (2022b). *Progress on the investigation phase of a digital euro*. https://www.ecb.europa.eu/euro/digital_euro/progress/shared/pdf/ecb.degov220929.en.pdf

European Central Bank. (2022c, December 8). *End-user on-boarding and digital euro access*. https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf//ecb.degov221208_item2onboardingaccessmag.en.pdf

European Central Bank. (2022d). *Digital euro glossary*. https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf/ecb.dedocs220420.en.pdf

European Central Bank. (2023a, October 18). *Eurosystem proceeds to next phase of digital euro project*. https://www.ecb.europa.eu/press/pr/date/2023/html/ecb.pr231018~111a014ae7.en.html

European Central Bank. (2023b). *Summary of the digital euro prototype* (Publication No. 2023/05/26). https://www.ecb.europa.eu/pub/pdf/other/ecb.prototype_summary20230526~71d0b26d55.en.pdf

European Central Bank. (2023d). *A stocktake on the digital euro*. https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf/ecb.dedocs231018.en.pdf

European Central Bank. (2023e, November 30). *ECB selects "European culture" and "Rivers and birds" as possible themes for future euro banknotes*. https://www.ecb.europa.eu/press/pr/date/2023/html/ecb.pr231130~cad7fa27ab.en.html

European Central Bank. (2023f). *Digital euro safeguards – Protecting financial stability and liquidity in the banking sector* (ECB Occasional Paper No. 346). https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op346~3b4318a919.en.pdf

European Central Bank. (2024a). *Technical note on the provision of multiple digital euro accounts to individual end users*. https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf/ecb.degov240325_digital_euro_multiple_accounts.en.pdf

European Central Bank. (2024b). *Progress on the preparation phase of a digital euro*. https://www.ecb.europa.eu/euro/digital_euro/progress/shared/pdf/ecb.deprp202406.en.pdf

European Central Bank. (2024c). *Update on the work of the digital euro scheme's Rulebook Development Group*. https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf/ecb.degov240103_RDG_digital_euro_schemes_update.en.pdf?f8e154918d3e5e25736dbf5b3edbaf05

European Central Bank. (2024d). *State of play on offline digital euro: 11th ERPB technical session on digital euro*. https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf/ecb.degov240411_item3updateofflinedigitaleuro.en.pdf

European Central Bank. (2024e, June 13). *Making the digital euro truly private*. https://www.ecb.europa.eu/press/blog/date/2024/html/ecb.blog240613~47c255bdd4.en.html

European Central Bank. (2024f, January 17). *One step ahead: Protecting the cyber resilience of financial infrastructures*. https://www.ecb.europa.eu/press/key/date/2024/html/ecb.sp240117~3e839b396f.en.html

European Commission. (2022). *Consultation on a digital euro*. https://finance.ec.europa.eu/regulation-and-supervision/consultations/finance-2022-digital-euro_en

European Commission. (2023a). Proposal for a regulation of the European Parliament and of the council on the establishment of the digital euro. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0369

European Commission. (2023b). *Impact assessment report*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023SC0233

European Parliament and Council of the European Union. (2015). *Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market*. Official Journal of the European Union, L 337, 35-127. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L2366

European Systemic Risk Board. (2020). *Systemic cyber risk*. https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf

European Union. (2018). *Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law*. Official Journal of the European Union, L 284, 22-30. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018L1673

European Union Agency for Cybersecurity (ENISA). (2023). *ENISA threat landscape 2023*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Europol. (2023a). *Internet organised crime threat assessment (IOCTA)*ENISA

Europol (2023b), ChatGPT - The impact of Large Language Models on Law Enforcement, a Tech Watch Flash Report from the Europol Innovation Lab, Publications Office of the European Union, Luxembourg.

Fang, F., Ventre, C., Basios, M., Kanthan, L., Martinez-Rego, D., Wu, F., & Li, L. (2022). Cryptocurrency trading: a comprehensive survey. *Financial Innovation*, *8*(1), 1-59.

Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, *10*(1), 11-36.

Florackis, C., Louca, C., Michaely, R., & Weber, M. (2023). Cybersecurity Risk. *The Review of Financial Studies*, *36*(1), 351–407. https://doi.org/10.1093/rfs/hhac024

Fung, B. S., & Halaburda, H. (2016). Central bank digital currencies: a framework for assessing why and how. *Available at SSRN 2994052*.

Galinec, D., & Steingartner, W. (2017, November). Combining cybersecurity and cyber defense to achieve cyber resilience. In *2017 IEEE 14th International Scientific Conference on Informatics*, 87-93.

Garg, S., Gentry, C., Sahai, A., & Waters, B. (2013). Witness encryption and its applications. In *Proceedings of the forty-fifth annual ACM symposium on Theory of computing* (pp. 467-476).

Garratt, R., & Lee, M. J. (2021). *Monetizing privacy* (No. 958). Staff Report.

General Data Protection Regulation (GDPR), Regulation (EU) 2016/679. (2016). *Official Journal of the European Union*. L 119, 1-88. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

Gellert, R. (2018). Understanding the notion of risk in the General Data Protection Regulation. *Computer Law & Security Review*, *34*(2), 279-288.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in computer virology*, *2*, 13-20.

Harvey, S. J. (2013). Smart meters, smarter regulation: Balancing privacy and innovation in the electric grid. *UCLA L. Rev.*, *61*, 2068.

Hasham, S., Joshi, S., & Mikkelsen, D. (2019). Financial crime and fraud in the age of cybersecurity. *McKinsey & Company*, *2019*.

Indrawati, F. A. (2023). An Ideal Legal Tender For The Digital Era. *Journal of Central Banking Law and Institutions*, *2*(3), 373-400.

Jabbar, A., Geebren, A., Hussain, Z., Dani, S., & Ul-Durar, S. (2023). Investigating individual privacy within CBDC: A privacy calculus perspective. *Research in International Business and Finance*, *64*, 101826.

Kakebayashi, M., Presto, G. P., & Yuyama, T. (2023, May). Policy Design of Retail Central Bank Digital Currencies: Embedding AML/CFT Compliance. In *International Conference on Financial Cryptography and Data Security* (pp. 216-244). Cham: Springer Nature Switzerland.

Kahn, C. M. (2018). Payment systems and privacy.

Khiaonarong, T., & Humphrey, D. (2019). Cash use across countries and the demand for central bank digital currency. *Journal of Payments Strategy & Systems*, *13*(1), 32-46.

Kiff, J., Alwazir, J., Davidovic, S., Farias, A., Khan, A., Khiaonarong, T., Malaika, M., Monroe, H. K., Sugimoto, N., Tourpe, H., & Zhou, P. (2020). A Survey of Research on Retail Central Bank Digital Currency, *IMF Working Papers*, *2020*(104), A001. Retrieved Jan 30, 2024, from https://doi.org/10.5089/9781513547787.001.A001

Kortvedt, H., & Mjolsnes, S. (2009, November). Eavesdropping near field communication. In *The Norwegian Information Security Conference (NISK)* (Vol. 27, p. 5768).

Laboure, M., H.-P. Müller, M., Heinz, G., Singh, S., & Köhling, S. (2021). Cryptocurrencies and cbdc: The route ahead. *Global Policy*, *12*(5), 663-676.

Lannquist, A., Warren, S., & Samans, R. (2020, January). Central bank digital currency policy-maker toolkit. In *Insight Report, World Economic Forum, Geneva*.

Lastra, R. M., & Allen, J. G. (2018). Virtual currencies in the Eurosystem: challenges ahead.

Lee, D. K. C., Yan, L., & Wang, Y. (2021). A global perspective on central bank digital currency. *China Economic Journal*, *14*(1), 52-66.

Leonov, P. Y., Vorobyev, A. V., Ezhova, A. A., Kotelyanets, O. S., Zavalishina, A. K., & Morozov, N. V. (2021, May). The main social engineering techniques aimed at hacking information systems. In *2021 Ural symposium on biomedical engineering, radioelectronics and information technology (USBEREIT)* (pp. 0471-0473). IEEE.

Levi, M., & Reuter, P. (2006). Money laundering. *Crime and justice*, *34*(1), 289-375.

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176-8186.

Lloyd, M. (2022). The future of money: central bank digital currencies. *Atlantic Economic Journal*, *50*(3), 85-98.

Masciandaro, D. (2018). Central Bank digital cash and cryptocurrencies: insights from a new Baumol–Friedman demand for money. *Australian Economic Review*, *51*(4), 540-550.

Mahari, R., Hardjono, T., & Pentland, A. (2022). AML by Design: Designing a Central Bank Digitalcurrency to Stifle Money Laundering. *MIT Science Policy Review*, *3*, 57-65.

Mbanaso, U. M., & Dandaura, E. S. (2015). The cyberspace: Redefining a new world. *IOSR Journal of Computer Engineering*, *17*(3), 17-24.

McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. *Summary of key findings and implications. Home Office Research report*, *75*, 1-35.

Mersch, Y. (2020, May 11). *An ECB digital currency – a flight of fancy?* [Speech]. European Central Bank. https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp200511~01209cb324.en.html

Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The role of user behaviour in improving cyber security management. *Frontiers in Psychology*, *12*, 561011.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* White paper.

Náñez Alonso, S. L., Echarte Fernández, M. Á., Sanz Bas, D., & Kaczmarek, J. (2020). Reasons fostering or discouraging the implementation of central bank-backed digital currency: A review. *Economies*, *8*(2), 41.

National Cyber Security Centre (NCSC). (2015). *Cybersecuritybeeld Nederland 2015 (CSBN 2015)*. https://www.ncsc.nl/document/cybersecuritybeeld-nederland-2015

National Cyber Security Centre (NCSC). (2021). *Cyber security assessment Netherlands 2021 (CSAN 2021)*. https://www.ncsc.nl/cyber-security-assessment-2021

NIST (n.d.). Privacy risk venn diagram. https://www.nist.gov/image/privacy-risk-venn-diagram

Ocaka, A., Briain, D. Ó., Davy, S., & Barrett, K. (2022, April). Cybersecurity threats, vulnerabilities, mitigation measures in industrial control and automation systems: a technical review. In *2022 Cyber Research Conference-Ireland (Cyber-RCI)* (pp. 1-8). IEEE.

Panetta, F. (2020, October 12). *A digital euro for the digital era.* [Speech]. European Central Bank. https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp201012_1~1d14637163.en.html

Panetta, F. (2021, December 10). *The present and future of money in the digital age.* [Speech]. European Central Bank. https://www.ecb.europa.eu/press/key/date/2021/html/ecb.sp211210~09b6887f8b.en.html

Panetta, F. (2022, September 26). *Demystifiyng wholesale central bank digital currency*. [Speech]. European Central Bank. https://ecb.europa.eu/press/key/date/2022/html/ecb.sp220926~5f9b85685a.en.html

Passacantando, F. (2021). The digital euro: challenges and opportunities. *The (Near) Future of Central Bank Digital Currencies*, *113*.

Pfitzmann, A., & Hansen, M. (2010). A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management.

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & security*, *31*(4), 597-611.

Politou, E., Alepis, E., & Patsakis, C. (2019). Profiling tax and financial behaviour with Big Data under the GDPR. *Computer law & security review*, *35*(3), 306-329.

Purtova, N. (2022). From knowing by name to targeting: the meaning of identification under the GDPR. *International Data Privacy Law*, *12*(3), 163-183.

Queen Máxima. (2022, October 14). *Speech at the IMF event "CBDC and financial inclusion: Risks and rewards" at the annual meetings of the IMF and World Bank in Washington, DC*. Royal House of the Netherlands. https://www.royal-house.nl/documents/speeches/2022/10/14/speech-of-queen-maxima-at-the-imf-event-cbdc-and-financial-inclusion-risks-and-rewards-at-the-annual-meetings-of-the-imf-and-worldbank-in-washington-dc

Rahman, A. A. (2022). A Decentralized Central Bank Digital Currency.

Rauchs, M., Glidden, A., Gordon, B., Pieters, G. C., Recanatini, M., Rostand, F., ... & Zhang, B. Z. (2018). Distributed ledger technology systems: A conceptual framework. *Available at SSRN 3230013*.

Rennie, E., & Steele, S. (2021). Privacy and emergency payments in a pandemic: How to think about privacy and a central bank digital currency. *Law, Technology and Humans*, *3*(1), 6-17.

Riccardi, M., & Levi, M. (2018). Cash, crime and anti-money laundering. *The Palgrave handbook of criminal and terrorism financing law*, 135-163.

Sasse, M. A., & Flechais, I. (2005). Usable security: Why do we need it? How do we get it?. O'Reilly.

Sai, A. R., Buckley, J., & Le Gear, A. (2019, March). Privacy and security analysis of cryptocurrency mobile applications. In *2019 fifth conference on mobile and secure services (MobiSecServ)* (pp. 1-6). IEEE.

Selzer, A. (2021). The appropriateness of technical and organisational measures under article 32 gdpr. *European Data Protection Law Review (EDPL), 7(1),* 120-128.

Sethaput, V., & Innet, S. (2023). Blockchain application for central bank digital currencies (CBDC). *Cluster Computing*, 1-15.

Shahzad, R. K., & Lavesson, N. (2011). *Detecting scareware by mining variable length instruction sequences* (pp. 1-8). IEEE.

Sharman, J. C. (2009). Privacy as roguery: Personal financial information in an age of transparency. *Public Administration*, *87*(4), 717-731.

Shastri, S., Wasserman, M., & Chidambaram, V. (2019). The seven sins of {Personal-Data} processing systems under {GDPR}. In *11th USENIX Workshop on Hot Topics in Cloud Computing (HotCloud 19)*.

Shehu, A. Y. (2012). Promoting financial inclusion for effective anti-money laundering and counter financing of terrorism (AML/CFT). *Crime, law and social change*, *57*(3), 305-323.

Sidorenko, E. L., Sheveleva, S. V., & Lykov, A. A. (2021). Legal and economic implications of central bank digital currencies (CBDC). In *Economic Systems in the New Era: Stable Systems in an Unstable World* (pp. 496-502). Springer International Publishing.

Singh, A., & Gupta, B. B. (2022). Distributed denial-of-service (DDoS) attacks and defense mechanisms in various web-enabled computing platforms: issues, challenges, and future research directions. *International Journal on Semantic Web and Information Systems (IJSWIS)*, *18*(1), 1-43.

Soderberg, G., Bechara, M. M., Bossu, W., Che, M. N. X., Davidovic, S., Kiff, M. J., ... & Yoshinaga, A. (2022). Behind the scenes of central bank digital currency: Emerging trends, insights, and policy lessons.

Strupczewski, G. (2021). Defining cyber risk. *Safety science*, *135*, 105143.

Tatlı, E. I. (2015). Cracking more password hashes with patterns. *IEEE Transactions on Information Forensics and Security*, *10*(8), 1656-1665.

Tobin, J. (1987). A case for preserving regulatory distinctions. *Challenge*, *30*(5), 10-17.

Toch, E., Bettini, C., Shmueli, E., Radaelli, L., Lanzi, A., Riboni, D., & Lepri, B. (2018). The privacy implications of cyber security systems: A technological survey. *ACM Computing Surveys (CSUR)*, *51*(2), 1-27.

Tronnier, F., Harborth, D., & Hamm, P. (2022). Investigating privacy concerns and trust in the digital Euro in Germany. *Electronic Commerce Research and Applications*, *53*, 101158.

Tronnier, F., Recker, M., & Hamm, P. (2020). Towards Central Bank Digital Currency–A Systematic Literature Review.

Tzanou, M. (2013). Data protection as a fundamental right next to privacy?'Reconstructing' a not so new right. *International Data Privacy Law*, *3*(2), 88-99.

United Nations. (1948). Universal Declaration of Human Rights.

Urbinati, E., Belsito, A., Cani, D., Caporrini, A., Capotosto, M., Folino, S., Galano, G., Goretti, G., Marcelli, G., Tiberi, P. & Vita, A. (2021). *A digital euro: a contribution to the discussion on technical design choices* (No. 10). Bank of Italy, Directorate General for Markets and Payment System.

Van den Berg, B., Prins, R., & Kuipers, S. (2021). Assessing contemporary crises: Aligning safety science and security studies. In *Oxford Research Encyclopedia of Politics*.

Van den Berg, J., van Zoggel, J., Snels, M., van Leeuwen, M., Boekee, S., Koppen, L., van den Berg, B., de Bos, A., & van der Lubbe, JCA. (2015). On (the emergence of) cyber security science and its challenges for cyber security education.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97-102.

Vučinić, M., & Luburić, R. (2022). Fintech, risk-based thinking and cyber risk. *Journal of Central Banking Theory and Practice*, *11*(2), 27-53.

Wall, D. S. (2007), Cybercrime: The Transformation of Crime in the Information Age, Polity, London.

Wall, D. S. (2017). Crime, security and information communication technologies: The changing cybersecurity threat landscape and its implications for regulation and policing. *Security and Information Communication Technologies: The Changing Cybersecurity Threat Landscape and Its Implications for Regulation and Policing (July 20, 2017)*.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard law review*, 193-220.

Wenker, K. (2022). Retail central bank digital currencies (CBDC), Disintermediation and financial privacy: The case of the Bahamian sand dollar. *FinTech, 1*(4), 345-361.

Westermeier, C. (2020). Money is data–the platformization of financial transactions. *Information, Communication & Society*, *23*(14), 2047-2063.

Whitten, A., & Tygar, J. D. (1998). *Usability of security: A case study*. School of Computer Science, Carnegie Mellon University.

Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., ... & Platts, J. (2022). Cybersecurity, data privacy and blockchain: A review. *SN computer science*, *3*(2), 127.

Xu, J. (2022). Developments and Implications of Central Bank Digital Currency: The Case of China e-CNY. *Asian Economic Policy Review*, *17*(2), 235–250.

Yadav, T., & Rao, A. M. (2015). Technical aspects of cyber kill chain. In *Security in Computing and Communications: Third International Symposium, SSCC 2015, Kochi, India, August 10-13, 2015. Proceedings 3* (pp. 438-452). Springer International Publishing.

Yermack, D. (2013). *Is Bitcoin a real currency? An economic appraisal.* In Handbook of Digital Currency (pp. 31-43). Elsevier.

Zarsky, T. Z. (2015). The privacy-innovation conundrum. *Lewis & Clark Law Review*, *19*(1), 115-168.

Zhang, T., & Huang, Z. (2022). Blockchain and central bank digital currency. *ICT Express*, *8*(2), 264-270.

Zhang, X., Yadollahi, M. M., Dadkhah, S., Isah, H., Le, D. P., & Ghorbani, A. A. (2022). Data breach: analysis, countermeasures and challenges. *International Journal of Information and Computer Security*, *19*(3-4), 402-442.

Zouina, M., & Outtai, B. (2019). Towards a distributed token based payment system using blockchain technology. *International conference on advanced communication technologies and networking*, 1-10.