Master Thesis

Digital Euro vs Bitcoin: Trust-Fostering Design

MSc Business Administration and E-Business

Supervisor:

Jan Damsgaard

Submission Date:

15.11.2023

Number of standard pages:

102

Number of characters:

209,698

Authors:

Caroline Illum	132635	cail19ab@student.cbs.dk
Nanna Sunagawa Pedersen	155489	nape22ab@student.cbs.dk

Abstract

In the last decade we have seen a digital transformation of the financial industry. Bitcoin has emerged as a new form of payment, disrupting the traditional way of storing monetary value and conducting financial transactions. The benefits offered by the decentralized, peer-to-peer architecture of Bitcoin and other cryptocurrencies have garnered widespread popularity globally particularly in the Global South. Nevertheless, the level of trust and adoption in Bitcoin have been hindered by a number of drawbacks including Bitcoin's price volatility and lack of regulatory clarity. Central banks around the world have responded to the rapidly evolving financial landscape by introducing its own unique digital currency, known as Central Bank Digital Currencies (CBDCs). Presently, the European Central Bank (ECB) is investigating its own kind, namely the digital euro, that aims to be the digital equivalent of cash. Despite the ongoing research by the ECB, academic research on the potential trustworthiness of centralized digital currencies like the digital euro has not been adequately addressed. Further investigation is needed to understand how the digital euro can foster trust among users particularly in comparison to Bitcoin. This thesis therefore seeks to identify the trust factors (social, technical, institutional, economic, socio-technical) that are most important for the ECB to consider in the design of the digital euro through a 2-round Delphi study consisting of a panel of five industry experts. The study comprised an initial semi-structured interview round followed by a subsequent survey round with the aim of reaching consensus on the most important trust factors for the design of the digital euro, as well as to understand the underlying reasonings with regard to consensus and non-consensus reaching issues. The present study finds consensus on 10 trust factors that are crucial for the ECB to consider in designing the digital euro for trust. Additionally, the panelists identified volatility and reputation as the primary drawbacks of bitcoin, which are effectively addressed by the digital euro through its institutional support and backing that ensures its stability, as well as the pre-existing trust and credibility in the ECB that helps to enhance the digital euro's reputation. Based on the 10 trust factors, the present thesis recommends that the ECB should implement measures to ensure stability, adopt a privacy-by-design approach, allow for privacy-enabled low value transactions, ensure seamless UX/UI, and a hybrid account-based and token-based verification system.

Acknowledgements

We would like to express our deepest gratitude to our thesis supervisor, Professor Jan Damsgaard, for his mentorship, support and invaluable advice in the making of this thesis paper. We also thank the interview participants for taking part in the thesis and allowing us to benefit from their knowledge and expertise.

Table of contents

Table of figures

Table of tables

1. Introduction

Trust has served as a fundamental pillar in the functioning of monetary systems throughout history and in modern times. Its influence is pervasive in our monetary system, evident in various aspects, from the inscription of the U.S dollar bill stating, "In God we trust" and even deeply embedded in the etymology of the word "credit" which traces its roots to the Latin word, *credere*, meaning "to believe." A tangible embodiment of this trust in monetary systems is cash, which has earned its confidence through its backing by the state and the central bank, in addition to its role in facilitating fast, reliable and private peer-to-peer transactions. However, as financial transactions become increasingly digital, paper money is becoming less prevalent as a means of transaction in parts of Europe like Sweden (Sveriges Riksbank, 2023). On the other hand, electronic and digital payment methods are gaining increasing prominence, with traditional fiat currencies like Dollars and Euros being replaced by digital currencies.

One such currency is Bitcoin, which has gained popularity as the first decentralized cryptocurrency. Bitcoin is a peer-to-peer electronic currency that operates on a decentralized technology called blockchain. This electronic cash-like currency has distinct advantages that are difficult for traditional fiat currencies to rival. These advantages include transparency, global accessibility, and the absence of centralized third-party intermediaries. The global financial crisis of 2008-9 and the subsequent abuse of monetary policies such as the unprecedented rate of money printing by the central bank have sparked concerns about the trustworthiness of traditional fiat currencies and financial institutions. Bitcoin has emerged as an alternative currency and asset that aims to address these concerns by providing a decentralized, *trustless* monetary system that is independent of any financial intermediaries.

In response, governments and central banks around the world have begun experimenting with their own form of digital currency known as central bank digital currencies (CBDCs), such as the Digital Euro, to modernize their monetary systems and to potentially enhance public trust in existing financial institutions. Furthermore, the dwindling of cash usage has urged governments

to consider the implementation of "cash-like" digital currencies, namely CBDCs, to meet the evolving needs of their citizens in an increasingly digitalized society.

The increasing digitalization of currencies calls into question the evolving nature of trust in monetary and financial systems. Since the emergence of central banks in England in the 17th century, governments and central banks have been the primary entities responsible for issuing and regulating national currencies. In doing so, these entities have sought to foster public trust and confidence in their currencies, as public trust in the nation's currency is crucial for the smooth functioning of the economy (European Central Bank 2020; Arrow 1972). Users of currencies must trust that the currency that they hold will be accepted in exchange for a good or service by other parties. The abandonment of the gold standard in the 20th century has reemphasized the significance of ensuring public confidence in the long-term stability and worthiness of a currency. The traditional trust associated with fiat currencies no longer stems from a guarantee that they are redeemable for an equivalent value in gold. Rather, we now rely on the assurance that central banks will responsibly manage and maintain the value of our money without engaging in manipulation, deflationary practices, or inflationary measures.

As we progress towards an era of digitalized currency, the concept of tryst undergoes a profound transformation, as exemplified by Bitcoin’s trustless and decentralized architecture. Given the increasing prominence of cryptocurrencies, the question of how exactly the European Central Bank should seek to establish trust in the Digital Euro as a dependable and secure currency loom as a central and intriguing topic worth investigating.

1.1 Research Question

The research question that this thesis seeks to investigate emerges from the backdrop of these transformations. Bitcoin, which has amassed 219 million owners, has redefined how trust operates in the world of digital finance. This research seeks to shed light on the mechanisms and strategies that CBDCs employ in the pursuit of trustworthiness, compared to the decentralized and

trustless nature of Bitcoin. This paper investigates the Digital Euro and Bitcoin, and investigates the following research question based on the research context outlined above (RQ):

How does the digital euro seek to foster trust and confidence compared to Bitcoin?

Due to the breadth of this research question, the following three sub-questions will be explored to provide a comprehensive analysis:

Sub-RQ 1: *"How and what mechanisms establish trust and confidence in digital currencies?"*

The objective of the Sub-RQ 1 is to understand and lay the theoretical groundwork on how trust in digital currencies is established. This will be accomplished through a review of relevant existing literature on the concept of trust and confidence in relation to digital currencies including CBDCs and cryptocurrencies. Once the trust-promoting features and mechanisms of digital currencies are established, the following Sub-RQ 2 can be addressed:

Sub-RQ 2: *"What design characteristics should be considered or implemented to foster trust and confidence in the digital euro?"*

Based on the theoretical understanding of trust and confidence promoting features and characteristics of digital currencies, the goal of sub-RQ 2 is to identify specific design features and characteristics that are most relevant for ECB to consider in the design of the digital euro. The theoretical underpinnings of trust features in digital currencies identified in Sub-RQ1 will guide the exploration of Sub-RQ 2, and interviews with industry experts will confirm which trust and confidence promoting features are most relevant in the context of the digital euro. The answers to Sub-RQ2 will be enhanced through the exploration of Sub-RQ 3, which seeks to assess the extent to which the features identified will effectively address the risks associated with bitcoin that undermine its trustworthiness:

Sub-RQ 3: *"To what extent do the trust and confidence promoting characteristics of the digital euro address the risks associated with bitcoin that undermine its trustworthiness?"*

We will analyze and compare the recommended design choices of the digital euro from Sub-RQ 2 against the drawbacks of bitcoin. Exploring Sub-RQ 3 will further provide insights on the strengths and weaknesses of centralized digital currencies like the digital euro in fostering trust compared to decentralized digital currencies like bitcoin.

1.2 Research Motivation

The motivation for undertaking this research can be sub-divided into two factors: personal interest and research worthiness.

Personal interest

The authors' personal interests in the research question are deeply rooted. Nanna, with an academic background in international relations and business administration and e-business, has been fascinated by social, political and economic issues that impact global relations and the ever-evolving digital landscape. Nanna has observed the increasing significance of digital currencies, notably CBDCs and cryptocurrencies, in reshaping the financial world and challenging traditional notions of trust and authority, which are inherently political and social in nature. Caroline, with an academic background in communication science and business administration (e-business), has a strong interest in emerging technologies and their potential to bring positive disruption to both society and individuals. Her prior coursework and professional experience have introduced her to the concepts of blockchain technology, cryptocurrencies, and regulatory compliance, sparking her interest in how the landscape will evolve as CBDCs are introduced.

Research worthiness

Trust is a phenomenon that underpins a vast array of our political, social and economic activities. After all, these activities rely on human-to-human interactions and discourse, in which trust plays an indispensable role in navigating uncertainties. In the political sphere, public trust in government and intuitions is essential for effective implementation of public policies. Lack of public trust can lead to collapse of governance and political instability. In the social sphere, trust is the cornerstone of interpersonal relationships. Without trust, communities would struggle to cooperate and build a well-functioning and sustainable community. In the economic sphere, trust plays an integral role in driving effective and efficient trade, exchange of goods, services and information, investment decisions, influencing consumer behavior, and other economic activities. Lack of trust can lead to market failure and corruption.

The multifaceted nature of money, encompassing these three dimensions of trust, becomes evident through real life examples. In Argentina, hyperinflation has resulted in the local population losing trust in its local currency, the government, and the local economy, indicating degrading political and economic trust. This is paralleled by increasing adoption in cryptocurrencies. According to GWI research, Argentina now ranks second globally, with a 23.5 percent adoption rate, following Turkey at 27.1 percent, reflecting a shift in the landscape of trust in financial systems (Singh & Mattackal, 2023). More recently, the failure to achieve widespread adoption of Nigeria's local CBDC, the e-Naira, which had an adoption rate of less than one percent, underscores the imperative of trust in monetary acceptance and adoption (IMF, 2023, p. 23). We believe that these events warrant thorough research on the nexus between trust, the digital euro, and bitcoin, especially as the European Union gears up for the digital euro.

The current research contributes to the existing literature on the digital euro and bitcoin, and more broadly on CBDCs, cryptocurrencies and trust in payment systems by specifically focusing on the mechanisms and design characteristics that the digital euro plans to employ to foster public trust and confidence compared to bitcoin. There is value in this research considering that the decentralized finance space is gaining popularity and the potential for wide-scale adoption of cryptocurrencies like bitcoin is increasing. Whether CBDCs can compete with cryptocurrencies

like Bitcoin by offering a trustworthy digital currency that is more attractive for users and their needs will guide policy makers, central banks and stakeholders in their design considerations of the digital euro and other CBDCs. This research is also timely, considering that the digital euro and most other CBDCs are still in their development phase and yet to be launched.

Our personal interest in the research question has been validated by our literature review. By conducting a systematic literature review, we have gained valuable insights into the existing body of knowledge and identified areas of research significance. The literature review has also reinforced the importance and relevancy of our research question, as academic literature on the topic of public trust in CBDCs and bitcoin is an area of study and discourse that has been recently emerging as both CBDCs and bitcoin are relatively new innovations. This underscores the timeliness of our study and for our findings to contribute to the developing discourse on the topic.

1.3 Outline

This research paper is sectioned into eight main chapters: Introduction, Literature Review, Re-visiting the Research Question, Methodology, Theoretical Framework, Findings, Discussion and Conclusion.

The first introductory chapter provides a description of the RQ and the research motivation, which sets the research context of the present thesis. The second chapter details the systematic literature review, in which we demonstrate the systematic process employed to conduct the literature review including the utilized search strings, database selection, and search filtering choices made to locate relevant literature. The chapter also provides a summary of relevant literature based on three thematic areas: Trust and Confidence, Trust in Cryptocurrencies, and Trust in CBDCs. The third chapter is dedicated to reformulating the main RQ and sub-RQ 2 based on our literature review findings, setting the course of our research. Thereafter, chapter four details the research methodology, outlining the chosen research philosophy and design and its implications, as well as the methods employed in our data collection and analysis. Chapter five outlines the theoretical framework employed in our

deductive research design, serving as a guide for the data collection and analysis conducted in this thesis. Chapter 6 details the findings gathered from analyzing our research data, which lays the groundwork for answering the RQ and sub-RQs. Chapter seven provides recommendations for how the ECB should design the digital euro to ensure trust based on the findings detailed in the previous chapter. Limitations of the present thesis and suggestions for future research are also discussed. The final chapter concludes with a summary of our main findings and concrete answers to the main RQ and sub-RQs.

1.4 Conceptual Framework

The present section defines concepts that are closely related to the present thesis, and frequently referred to throughout the paper.

Central Bank Digital Currencies (CBDCs)

A CBDC is a digital version of a country's official currency that is issued and regulated by a central bank. It is a form of legal tender that functions as a direct liability of the central bank and is denominated in the national unit of account (Bank of International Settlements, 2020). There are two types of CBDCs – wholesale and retail - that are under development across most countries. Wholesale CBDCs are restricted to the use of financial institutions for the purposes of interbank settlements and wholesale payments (Bank of International Settlements, 2021c, p. 70). Retail CBDCs are expected to provide a cash-like digital payment system for the wider public, enabling individuals to electronically conduct everyday transactions, as well as access and store their monetary value through digital devices. CBDCs differ from cryptocurrencies like Bitcoin in three main aspects. CBDCs are issued and regulated by central banks; CBDCs are backed by the government; and central authorities guarantee CBDCs as a form of legal tender (Stanley, 2022; Karam, 2023).

Digital euro

The digital euro represents the CBDC form of the Euro, issued by the ECB. The digital euro is currently in the two-year investigation phase, in the ECB is exploring the technical and

policy options that will possibly serve as the foundation for the development of the digital euro (Central Bank of Ireland, n.d). As of date, the ECB has declared that the digital euro will serve as "an electronic equivalent of cash," offering an array of features including offline payments, free transactions, universally acceptance at all retail establishments, ensuring security and privacy akin to cash transactions, and maintaining a one-to-one parity with the euro, making it readily exchangeable and equivalent in value (European Central Bank, n.d.-b).

The ECB (n.d.-a) has articulated the introduction of a digital euro as a response to the changing preferences of consumers in the eurozone, who are increasingly favoring electronic payment methods over cash. Furthermore, the ECB underscores that the digital euro is essential for maintaining the eurozone's competitiveness in the face of non-European payment services providers who currently hold a dominant position within the European financial market (European Central Bank, n.d.-a).

Cryptocurrencies

Cryptocurrencies are digital forms of currency that operate on a decentralized technology called blockchain, which is a distributed ledger system that records all transactions across a network of computers. Unlike traditional currencies which are issued and controlled by central authorities, cryptocurrencies are typically decentralized, with limited control and influence from singular entities. Cryptocurrencies rely on cryptographic techniques to secure and validate peer-to-peer transactions, thereby upholding the integrity of blockchain network.

There are currently about 26,000 different types of cryptocurrencies in the market, each with unique features and functionalities (McGimpsey & Broverman, 2023). They entail an array of currencies, including bitcoin, altcoins and stablecoins, as well as digital assets that extend beyond traditional monetary functions such as security tokens that represent ownership of real-world assets and non-fungible tokens (NFTs) representing digital or physical items. Despite their varying use cases, their shared characteristic is their utilization of blockchain technology (ibid).

Bitcoin

Bitcoin is the first cryptocurrency created and launched in January 2009 by an entity under the pseudonym of Satoshi Nakamoto. Bitcoin is built on decentralized blockchain technology which facilitates direct, peer-to-peer transactions (Nakamoto, 2008). According to the bitcoin white paper, bitcoin embodies a "*trustless*" system, as it validates transactions with cryptographic technology, eliminating the need for centralized intermediaries to facilitate the execution and settlement of transactions (Nakamoto, 2008). The maximum supply of bitcoin is capped at 21 million, and the issuance of bitcoin is done through a process known as mining involving mathematical problem-solving.

As outlined in the Bitcoin white paper, Bitcoin was originally designed as an electronic payment system, mirroring the functionality of cash (Nakamoto, 2008, p. 1). However, since its inception, Bitcoin's use case has evolved to encompass both a medium of exchange as well as a digital asset for investment purposes (Saiedi et al., 2021; Budree & Nyathi, 2023). The present thesis considers Bitcoin in its original function as a payment system with the aim of conducting a comparative analysis in contrast to the digital euro.

2. Literature review

In this thesis, we conduct a systematic literature review to achieve the following four objectives: 1) Get a thorough overview of the current state of the literature; 2) examine how each of our concepts is analyzed within a broader theoretical context. 3) identify appropriate theories and models for further analysis, and 4) determine research gaps. The subsequent section provides an in-depth overview of how our systematic literature review has been conducted. We provide this overview to ensure full transparency of the process and to enable anyone to replicate it, as recommended by Fisch and Block (2018, p. 104).

Search parameters

According to Saunders et al. (2019, p. 70-1), the first step in devising a literature search strategy is to define the parameters within which the literature search will be conducted. Defining the parameters of a literature search entails being clear about the following parameters

based on the given research question: 1) language of publication; 2) subject area; 3) business sector; 4) geographical area; 5) publication period; 6) literature type. The search parameters of this thesis are illustrated in table 1. As proposed by Saunders et al. (ibid), we began by defining both a broad and narrower set of search parameters based on our preliminary understanding of the subject matter of our research question. The purpose of both the narrow and broader parameters are to guide the search of our literature, starting with narrow parameters and broadening one or more parameters in the case that narrow search parameters did not yield the desired search findings. These parameters were revisited during the literature review based on the findings of our search.

Table 1: Literature search parameters

Parameter	**Narrow**	**Broader**
Language	UK and USA	UK and USA
Subject area	CBDCs Digital Euro Bitcoin Cryptocurrency Trust Confidence	Digital currency Cryptocurrency CBDCs Trust in financial systems Trust in payments Trust in money
Business sector	Digital currencies	Finance
Geographical area	Europe	Global
Publication period	Since 2008	Anytime
Literature type	Peer reviewed journals and books	Journals and books

Search terms

The second step of developing a literature search strategy is to identify relevant search terms which are keywords that will be used to search for relevant literature. We used the brainstorming technique suggested by Saunders et al. (2019, p. 73) to generate keywords that would be relevant for our literature search. The brainstorming technique was performed together by both authors of this thesis by first writing down a list of all words and phrases that we deemed relevant to our research question. Thereafter, we evaluated the list of keywords and narrowed down

the most relevant keywords, arriving at the following keywords: *digital euro, bitcoin, cryptocurrency, CBDC, central bank digital currencies, trust, confidence.* These keywords were noted down prior to formulating search strings and conducting our literature search on search databases.

Databases and search strings

When performing a systematic literature review, Bramer et al. (2017) recommends using various databases. We therefore performed an extensive search across numerous databases, including CBS Libsearch, Google Scholar, and Google Search Engine, to obtain thorough coverage of our topic. As a second step in the literature review, we utilized the forward and backward snowballing method (Wohlin 2014). The former method was employed in Google Scholar which offers a feature to conveniently look for cited works. The latter method was employed by scanning the references of relevant articles in search of additional relevant literature. Additionally, we used an artificial intelligence tool called Connected Papers, which locates similar articles based on co-citation and bibliographic coupling (Smolyansky, 2020). This tool facilitated the discovery of seminal works within the realms of our research subjects, ensuring that we did not overlook any critical pieces that might not have been readily available in the library databases.

CBS Libsearch

When searching for relevant literature on CBS Libsearch, we employed a single search string utilizing Boolean logic, "AND" and "OR", taking advantage of the database's capability to support this type of search (see table 2). Upon initially retrieving 4,641 results, we filtered the search results using Boolean logic, "NOT", to exclude literature containing keywords that we deemed irrelevant to our research question, such as "healthcare" and "gambling". Additionally, we filtered the search results based on the narrow search parameters described in table 1, to retrieve literature in English, peer-reviewed articles, book chapters and conference documents between the publication time frame of the 1st of January 2008 to the 31st of December 2023. We decided to

filter the publication period starting from 2008 onwards, as this marks the emergence of Bitcoin. The final search amounted to 354 results, and each article was assessed based on its titles and abstract to determine its relevance to our research topic. Once completed, 28 relevant search results were identified.

Table 2: CBS Libsearch search results

CBS Libsearch search string	**Initial results**	**Filtered results**	**Selected results**
("digital euro" OR cbdc* OR "central bank digital currenc*" OR bitcoin OR crypto OR cryptocurrenc*) AND (trust* OR confidence*) NOT (mining OR "supply chain" OR 5g OR cbdca OR iot OR computation OR health OR nft OR stablecoin OR volatility OR gambling OR hash OR dao OR "smart contract" OR "artificial intelligence" OR miners OR healthcare OR oracle OR)	4641	354	28

Google Scholar

Google Scholar does not support the same type of extensive search query and Boolean logic capabilities as CBS Libsearch. Hence, we divided the search string using Boolean logic, "OR", into ten narrower searches (a selection can be found in table 3, with the remaining in appendix 6.1). Our criteria for the search were limited to English literature from 2008 onwards, with no restrictions placed on material type (e.g., articles and book chapters) and peer-reviewed

status due to Google Scholar's limitations. As a result, our Google Scholar search included both peer reviewed and non-peer reviewed materials, as well as all types of materials. This broader parameter was chosen to encompass potential new research on CBDCs that may not have yet been peer-reviewed, thus minimizing the risk of omitting any pertinent material given the relatively recent emergence of this subject.

The 10 search strings employed retrieved a significant number of filtered results (see table 3). Given the extensive volume of items retrieved, we needed to establish a screening strategy to determine when to halt the screening of these results. According to Webster and Watson (2002, p. 16), the objective of conducting a systematic literature search is to collect all pertinent literature to gain a comprehensive understanding of a topic. They propose that researchers should conclude their search when they no longer come across any new information. Furthermore, a guide published on Google Scholar by Griffith University (2021) highlights two prevalent approaches for filtering Google Scholar results. The initial approach involves limiting the screening to only the first x results, while the second strategy is to end the screening process if no new relevant items are discovered after reviewing several consecutive pages. Following this guidance, we concluded the screening process after reviewing 10 consecutive pages without finding any new relevant articles. In total, we found 28 relevant results across all 10 search strings.

Table 3: Google Scholar search results (see appendix 6.1 for full table)

Google Scholar search strings	**Initial results**	**Filtered results**	**Selected results**
1. confidence "digital euro" OR cbdc OR "central bank digital currency"	3.560	3.460	1
2. confidence bitcoin OR crypto OR cryptocurrency	103.000	28.200	0
3. trust "digital euro" OR cbdc OR	6140	5800	8

"central bank digital currency"			
4. trust bitcoin OR crypto OR cryptocurrency	232000	43600	4

Google Search Engine

The third database used to supplement the searches conducted on CBS Libsearch and Google Scholar was the Google search engine on 'Google.com'. After scanning relevant literature identified through CBS Libsearch and Google Scholar, we realized that pertinent secondary data such as reports published by third parties such as the European Central Bank, the Bank of International Settlements, International Monetary Fund and consulting firms on the subject matters of the Digital Euro, CBDCs, Bitcoin and Cryptocurrencies were not appearing in the results of academic library databases. We therefore conducted a literature search on the Google search engine using the previously identified keywords. We also supplemented the keywords used in the previous literature searches with additional keywords, including "ECB" and "bank of international settlements" to control the range of cites retrieved on the Google database, as per the recommendations of Saunders et al. (2019, p. 84). Additionally, we also utilized the search engines in the library database on the ECB website and BIS website, which allowed us to scan and identify relevant publications by the ECB and BIS. Although these reports that are retrieved from the internet search engine are not peer-reviewed, we decided to include them in our literature review as they provide valuable information and the most recent updates regarding the Digital Euro and CBDCs which are still in its nascent stages of research and development. This complements the peer-reviewed literature found in the library databases.

2.1 Literature selection and evaluation

The process for selecting relevant literature from the search results of the aforementioned databases adhered to the assessment criteria outlined by Saunders et al. (2019, p. 87-8). Papers that addressed the Digital Euro in connection with the themes of trust and confidence were given

priority and were considered highly relevant during the selection process because they closely pertained to our research question.

2.2 Trust and confidence

There is no universally accepted definition of trust in academic literature due to its multifaceted nature (Sas & Khairuddin, 2015, p. 2; Amaral et al., 2019; Viljanen, 2005, p. 175). However, Gambetta (1988) is commonly referred to by scholars as a foundational starting point for understanding the theoretical aspects of trust. According to Gambetta (1988), trust is defined as the subjective probability assessment performed by one party when engaging in an action with another party. This definition acknowledges that trust is a relationship involving a certain degree of risk. Similarly, Arrow's (1972) definition of economic trust posits that trust is a fundamental element in any commercial transaction, especially in situations where uncertainty and risk are involved. Under high trust, transaction costs are reduced, and negotiation efficiency is fostered (Dyer & Chu 2003, p. 59). While the notion of risk appears frequently in definitions of trust, a clear conceptualization is lacking, to which Amaral et al. (2019) have proposed a Reference Ontology of Trust (ROT), which describes trust as encompassing several characteristics besides risk, such as it being context-dependent, a cognitive belief of the trustor about the trustee's behavior, and the trustee being either an agent (person or object) or agentless (social systems, such as the financial system) (ibid).

In defining *trust*, De Filippi et al. (2020, p. 4) underscores the need to clearly distinguish between "*trust*" and "*confidence*", as they are often conflated or used interchangeably in scholarly discourse. Viljanen (2005, p.183) posits that confidence is an element of trust relations that influences the trustworthiness of the trustee but does not offer a clear and measurable definition of confidence. De Filippi et al. (2020, p. 4) points to prior literature to argue that whilst trust involves personal vulnerability and risk, confidence does not; instead, it stems from cognitive assurance based on past experiences that a person or system will perform as expected (De Filippi et al., 2020, p. 4). This explains why trust has received wider scholarly attention and theoretical contributions, as trust entails observable actions or communication by parties involved in establishing a trust-

based relationship whilst confidence is a psychological quality that is challenging to identify (De Filippi et al., 2020, p. 5; Jalava, 2003, p.184; Amaral et al., 2022).

In the domain of information systems (IS), trust has been contextualized within the framework of technological acceptance, adoption and usage (McKnight et al., 2002; Lankton et al., 2014; Lankton et al., 2015; Pavlou 2003; Kim et al., 2010; Zhang & Zhang, 2005; Tsiakis & Sthephanides, 2005). Kim et al. (2010) demonstrate that perceived security risks are positively correlated with perceived trust and the intention to use e-payment systems. Pavlou (2003) looked at consumer acceptance of e-commerce by integrating trust and perceived risk with the technology acceptance model (TAM), which theorizes that perceived ease of use and perceived usefulness are determinants of technology adoption (Davis, 1986). They found that trust factors including integrity, benevolence and competence of the transaction medium are antecedents of perceived risk, perceived usefulness and perceived ease of use of Web retailers (Pavlou, 2003). Similarly, Matemba and Li (2018) looked at the adoption of WeChat by integrating trust, security and privacy concerns with TAM, and found that trust is one of the most influential factors in driving WeChat adoption.

More recent IS discourse has emphasized the importance of differentiating *technological trust* from *human (social) trust* factors, whereby the former is based on system-like trust constructs like *reliability*, *functionality* and *helpfulness* while social trust refers human-like trust factors that characterizes interpersonal trust relations like *integrity*, *credibility*, *benevolence* (McKnight et al., 2011; Vance et al., 2008; Lankton et al., 2015). Institutional trust theory by Luhmann (1979,1986) has also been applied in various IS studies, which argues that trust in the legal system is what allows for strangers to engage in contracts. McKnight and Chervany (2001) argue that institutional trust strengthens interpersonal trust as institutional mechanisms offer protection against uncertainties of trusting another party. However, this does not mean that they are mutually exclusive. Leppanen (2010, p.28) contends that social, institutional and technological trust factors should all be considered in tangent when studying trust in technology. For instance, McKnight et al. (2011) considered propensity to trust in technology, individual technology trusting beliefs (reliability, functionality and helpfulness) and institutional trust factors as constructs to study trust

in technology and found significant influence amongst the constructs in overall post-adoptive IT use.

Trust models and theories in the IS discipline have also lent themselves to research on digital currencies. For example, Zarifis et al. (2014; 2015) developed a Digital Currency Trust Model which draws on e-commerce trust constructs identified by McKnight et al. (2002). They argue that trust measures in e-commerce like institution-based trust and interpersonal trusting beliefs about a Web retailer parallels that of trust in digital currencies (Zarifis et al., 2015). However, scholars outside of the IS domain like Tronnier et al. (2023) argue that applying IS-based trust models to digital currencies is flawed, as digital currencies are not merely technologies but monetary systems. Tronnier et al. (2022) point to Wonneberger and Mieg (2012) who identified 12 trust-related features of currencies based on a literature review of trust in monetary systems, which are divided into 3 sub-groups: hard, soft and idealistic trust factors. The authors argue that these trust factors, such as liquidity, security, and backing, vary in their trustworthiness depending on the type of currency. Amaral et al. (2022) have adapted the ROT to study CBDC ecosystem, demonstrating that trust does not solely emanate from beliefs from the trustor, but that the trustee can display qualities that signal trustworthiness, such as the existence of cybersecurity policy and the inclusion of minimum usability requirements.

In light of the above literature review on trust, we define trust as a *psychological state emanating from a context involving risk or uncertainty which mediates exchanges between two parties based on characteristics within the trustor, trustee and/or the environment.* Additionally, we depart from the orthodox approach described by McKnight et al. (2011) to studying trust solely through human characteristics from the trustor's perspective by incorporating an array of trust-related theoretical contributions noted above, including human (social), technical, institutional, and monetary trust theories (Zarifs et al., 2015; Wonneberger and Mieg, 2012; Amaral et al., 2022; Leppanen, 2010). This approach is better suited for our research question which looks at a trustor (the digital euro and bitcoin) that embodies technical, institutional and monetary features, which is to be trusted by humans. Furthermore, considering that the digital euro has not been released to the public, confidence is less suited for the present research as it is a cognitive expectation about

performance that is difficult to measure, whereas trust or trustworthiness of the digital euro can more easily be studied through its perceptible and tangible characteristics (De Filippi et al., 2020, p. 5; Jalava, 2003, p.184).

2.3 Trust in Cryptocurrencies

The relationship between trust and cryptocurrencies was first explored by Satoshi Nakamoto (2008) in the Bitcoin White Paper, in which the notion of trust was mentioned in the context of creating a peer-to-peer electronic cash system that eliminates the need for trusted third parties. Nakamoto (2008, p. 1) proposed that by relying on cryptographic mechanisms, the need for trust could be eliminated. However, scholarly research on trust in cryptocurrencies have countered this notion, arguing that despite the decentralized architecture of bitcoin, trust continues to play a crucial role in the adoption and usage of cryptocurrencies (De Filippi et al., 2020; Marella et al., 2020; Toufaily 2022; Auinger and Riedl 2018; Elsokkary et al., 2022). Yet, Jacobs (2021) contends that the lack of a clear consensus amongst scholars on the meaning and underlying assumptions of "trust" has led to diverging depiction of trust relationships with cryptocurrencies. This observation was also made in our systematic literature review on trust in cryptocurrencies, and the varying conceptualizations are detailed below.

Firstly, technological trust factors underlying cryptocurrencies have been identified by Ali et al. (2023) through interviews with blockchain users, in which they identified trust characteristics pertaining to technical, functional and valuableness of the technology. Similarly, De Filippi et al. (2020) posits that cryptographic rules, mathematics, and game-theoretical incentives are cornerstones of trust in blockchain, which they define as confidence that the technology will operate reliably and without fail. Marella et al. (2020) identified openness, immutability and security as trust-related technological attributes that are unique to blockchain-based cryptocurrencies. Toufaily (2022) developed a framework of trust towards crypto-token applications, which comprise of environmental, end-user, DApp, and technology characteristics. The latter pertained to blockchain technology characteristics, such as scalability, security and

privacy, which were found to affect users' trust in crypto-tokens (Toufaily 2022). In their study on motivations behind bitcoin users in Malaysia, Sas and Khairuddin (2017) found that technological characteristics of blockchain such as decentralization and cryptography to be strong sources of users' trust in bitcoin.

Non-technical trust factors from the users' perspective are also found to be equally as important in driving the adoption and usage of cryptocurrencies. Based on a literature review of bitcoin and trust in HCI, Sas and Khairuddin (2015) identified technological, social and institutional trust factors. Social trust refers to the interpersonal trust between bitcoin stakeholders, including users, miners, merchants and exchanges (Sas and Khairuddin 2015; Shcherbak 2014). The importance of interpersonal trust is also underscored by Lustig and Nardi (2015), positing that trust in bitcoin is distributed through socio-technical mechanisms. Through interviews with bitcoin users, they found that trust in service providers and vendors, as well as individual judgement of trustworthiness through experience (Lustig and Nardi 2015). Jalan et al.'s (2023) study on the effect of interpersonal trust on the adoption of Bitcoin, Ethereum and Litecoin found that societal trust, which they define as a generalized belief or expectation that people can be trusted, were positively correlated with interest in and adoption of cryptocurrencies.

Institutional trust relates to trust fostered by the governance and regulation of Bitcoin network and activities, such as public law, the consensus mechanism and protocols of the Bitcoin network, and trust in the open-source community (Sas and Khairuddin 2015). For instance, Lustig and Nardi (2015, p. 748-750) found that Bitcoin users trust cryptography over human authority but emphasized the need for human regulatory oversight to protect users against fraudulent behaviour. Auinger and Riedl (2018) conducted a literature review of IS literature on blockchain and found institutional trust to be equally important as technological trust factors. They argue that trust in the legislative system is the most important determinant influencing Bitcoin use, as users must be confident that potential issues can be addressed in a court of law. Albayati & Rho (2020) also found government regulation and individual experience accumulated through the use of cryptocurrencies had the largest effect on users' trust in cryptocurrencies.

Previous works on the relationship between trust and cryptocurrencies have also looked at the risks and drawbacks of cryptocurrencies in fostering trust. In the case of Bitcoin, the high degree of volatility in its value compared to other currencies has been identified as a barrier to trust and adoption among users and non-users of Bitcoin (Knittel et al., 2019; Marella et al., 2019, p. 266; Shahzad et al. 2018). The lack of regulation has also been identified as a barrier to trust in cryptocurrencies (Toufaily 2022; Shahzad et al., 2018). According to Shahzad et al. (2018), the uncertainty regarding the future of Bitcoin's regulatory landscape negatively impacts Bitcoin's price stability. Moreover, Bitcoin's pseudonymity is oftentimes misused to conduct illicit activity (Saiedi et al., 2021). In Toufaily's (2022, p. 7) interview with stakeholders in the cryptocurrency's ecosystem, respondents emphasized that privacy and anonymity of users as primary obstacles inhibiting both institutional and individual trust in blockchain technology and cryptocurrencies. Casino et al. (2019) have pointed to the privacy and confidentiality concerns of blockchains, as transactions are recorded on a public ledger despite user anonymization. Sas and Khairuddin (2017) interviewed nine Bitcoin users and found pseudo-anonymity to pose a significant issue in the context of their trust in the currency when using it to transact. Environmental factors, such as cultural resistance towards cryptocurrencies and electronic transactions, as well as the lack of institutional acceptance have also been found to be challenges affecting trust in cryptocurrencies (Toufaily, 2022, p.10). Finally, a barrier to trust in Bitcoin has also been attributed to the lack of technical knowledge among users (Akpaku, 2021; Sas and Khairuddin, 2015; Gao et al., 2016; Arli et al., 2020; Toufaily, 2022). However, Gao et al. (2016) also found a lack of technical understanding to be prevalent among Bitcoin users as much as non-users, but this was not a barrier to trusting and using the technology.

In sum, academic research on cryptocurrencies supports the notion that Nakamoto's (2008) concept of a "trustless" peer-to-peer network for Bitcoin is not an accurate depiction. Research in this field argues instead that trust has simply been redirected away from intermediaries to various other stakeholders in the blockchain-based ecosystem. The trust factors identified are technological, social (interpersonal), and institutional trust. Other miscellaneous factors such as

individual experiences have also been identified as drivers of trust in cryptocurrencies. On the other hand, several risks and drawbacks of bitcoin that undermine its trust have been identified and will be incorporated into our theoretical framework of this thesis (Table 5). These risks will be used as backdrop against assessing the extent to which the trust factors most relevant to trust in the digital euro will address these drawbacks of bitcoin. Furthermore, there has been a significant oversight in examining the various factors that influence monetary trust in relation to Bitcoin.

2.4 Trust in CBDCs

According to the IMF, the successful implementation of CBDCs will depend on sufficient public trust, which requires thorough design, policy and regulatory considerations (Georgieva 2022; Soderberg et al., 2023, p.17 & 26). Despite urgent calls for careful design considerations as means of building trust in CBDCs, research on the topic across academia, the ECB, and third-party policy makers are still scarce.

Design mechanisms to foster public trust in CBDCS have been proposed by the World Economic Forum which includes privacy, data protection, cybersecurity and resilience. Similarly, based on end-user consultations, the Bank of International Settlements (2021a, p. 6) has recommended six CBDC features: safety of funds, reduced (transaction) costs, offline payments, security, privacy and accessibility. However, trust is only discussed in relation to security, stating that user trust in the issuer, intermediaries and the technology are critical for the users' perception of security in CBDCs (ibid).

As for the digital euro, Finance Watch has most recently published a set of 7 recommendations for building trust in the digital euro, which include but are not limited to legal tender status, free transactions for users, data protection, and functionalities including offline payments (Stiefmüller, 2023). The ECB's first comprehensive report titled, "Report on a digital euro" (2020), also addresses trust in connection with user data privacy and security. It underscores the imperative requirement that the digital euro must be cyber resilient. The importance of integrating privacy

and security measures for trust has been echoed by previous studies research in the realm of CBDCs (Sandhu et al. 2023, Korfiatis, 2023; Gross et al., 2021; Tronnier et al., 2022; Tronnier & Kakkar, 2021) However, Tronnier et al.'s (2021) did not find that privacy concerns have a significant influence on behavioural intention to use the digital euro among Germans.

The importance of institutional trust in building public confidence in CBDCs is encapsulated in ECB president, Christine Lagarde's statement, in which she says that the role of the ECB is "to secure trust in money" (European Central Bank, 2020, p. 2). Likewise, Hyun Song Shin, economic adviser and head of research of the BIS, describes CBDCs as "anchored in the foundation of trust in the central bank." (Bank of International Settlements, 2021b). Within academic research, a recent study by Gupta et al. (2023, p. 9) on the relationship between perceived risk and benefits and CBDC adoption amongst users in India found that regulatory risk has a significant and negative correlation with adoption. Tronnier et al.'s (2021) study on the usage intention of digital euro amongst Germans found that trust in ECB has a significant influence on trust in the digital euro. Gross et al. (2021) proposes a design framework for CBDCs that offers fully private transactions and regulatory compliance, ensuring public trust is achieved in both aspects for a successful CBDC implementation. Bowler et al.'s (2023, p.12) work on design considerations for a non-custodial wallet for CBDCs also acknowledges that trust needs to be established through institutional and regulatory protection just like traditional centralized payments and which cryptocurrencies currently lack.

The ECB (2023, p. 7) has also highlighted the importance of interpersonal trust in developing a trustworthy digital euro, stating that only trusted intermediaries will be authorized to issue digital euro to the public, who are fully compliant with the law and legislation. The important role that trusted intermediaries play in driving CBDC adoption has been demonstrated by Ma et al., (2022) in which trust in merchants and providers of digital RMB payment system reduced the risk associated with using digital RMB.

Furthermore, monetary trust has also been discussed by the European Central Bank (2022, p. 3) by claiming that CBDCs will be a "monetary anchor" by fostering public confidence that private money to be convertible to CBDCs. The only academic study looking at monetary trust factors is Tronnier et al. (2022), in which they looked at hard trust factors derived from Wonneberger and Mieg (2021) such as liquidity, fungibility, and stability, and soft factors including credibility, image and security to assess the most influential trust factors in encouraging the use of the digital euro, and found that soft trust factors were more significant in influencing intention to adopt digital euro. Research on technological trust factors in relation to CBDCs are also lacking, and the only research thus far has been conducted by Soilen and Benhayoun (2021), who found that performance expectancy, which pertains to factors such as convenience, speed and service effectiveness, were found to be positively correlated with CBDC adoption.

Compared to research on trust in cryptocurrencies, CBDC as a research area is currently lacking in academic discourse and theoretical development. Our review of third-party policy proposals shows that robust proposals on trust-promoting mechanisms for CBDCs and the digital euro are still lacking. Academic research on CBDCs largely focuses on the drivers of adoption or intended use of CBDCs, and less so on the qualities of the currency that make it trustworthy as a form of payment. The most relevant and valuable contribution in this regard is Tronnier et al. (2022) who studied monetary trust factors and their effects on willingness to use CBDCs. We argue that this warrants further research for two reasons. First, hard trust factors were shown to not have a significant influence on privacy concerns, but our research objective is to assess the extent to which these hard trust factors are fulfilled by the digital euro and bitcoin, based on the assumption that public trust in currencies are fostered by central bank competencies. Secondly, our objective will be to interview industry experts whereby we assume that they have more knowledge of the extent to which these hard trust factors will be relevant, which will offer different perspective to Tronnier's (2022) findings from user interviews.

3. Revisiting the research question

In light of the literature review, the original RQ will be slightly adjusted to more accurately reflect the research gap that we aim to fill. The original RQ was worded as follows:

Original RQ: *How does the digital euro seek to foster trust and confidence compared to Bitcoin?*

We have decided to modify the original RQ by omitting the terms "does", "seek" and "confidence". Firstly, our original word choice "does" is in present tense, which assumes that there is rich academic research and policy proposals to base our analysis on how the digital euro seeks to establish trust. However, as our literature review chapter on trust in CBDCs has shown, this is not the case, as research on how CBDCs including the digital euro will garner trust is still in its nascent stages, which is not surprising considering that the ECB has only begun to announce its plans for developing a CBDC in 2020. For the same reasons, "seek" has been omitted for grammatical correctness.

Secondly, based on the definition on confidence as discussed in the literature review chapter on trust, we have decided to exclude confidence as a dependent variable of the trustworthiness of the digital euro and bitcoin. Since confidence is a cognitive state of mind based on past experiences, it is difficult to identify independent variables that would indicate whether the digital euro or bitcoin will be able to generate confidence. In comparison, the literature review has exemplified several trust factors such as technological, social, institutional and economic constructs that can influence the level of trustworthiness of a trustee. For this reason, this thesis will solely focus on trust as a dependent variable, however the extent to which the digital euro will be able to foster confidence will be discussed in relation to our findings of our data collection in the discussion section. Thus, the revised RQ is worded as follows:

Revised RQ: *How should the digital euro be designed to foster trust compared to bitcoin?*

Reformulating the original RQ led us to re-consider the value of exploring sub-RQ 2, since the objective behind the revised RQ and sub-RQ 2 are identical. To avoid any redundancy, we

have decided to exclude sub-RQ 2 from this thesis. The sub-RQs that we have decided to keep and explore for this thesis are the following:

Sub-RQ 1: *"How and what mechanisms establish trust in digital currencies?"*

Sub-RQ 2 (previously sub-RQ 3): *"To what extent do the trust characteristics of the digital euro address the risks associated with Bitcoin that undermine trust?"*

4. Methodology

This section will delineate the chosen methodology for this thesis that is best suited for addressing our RQ: *"How should the digital euro be designed to foster trust compared to bitcoin?"* The Research Onion model, proposed by Saunders et al. (2019), served as the starting point in determining the methodology. However, Melnikovas (2018, p. 34) contends that the Research Onion framework falls short in addressing research questions relating to future developments or phenomena. Given that the digital euro is still in its developmental phase, we adopt Melnikovas' (2018) solution of incorporating a second layer in the Research Onion framework, titled "approaches to futures research". Hence, Melnikovas' (2018) revised Research Onion framework with seven layers will guide our methodological approach (see Figure 1).

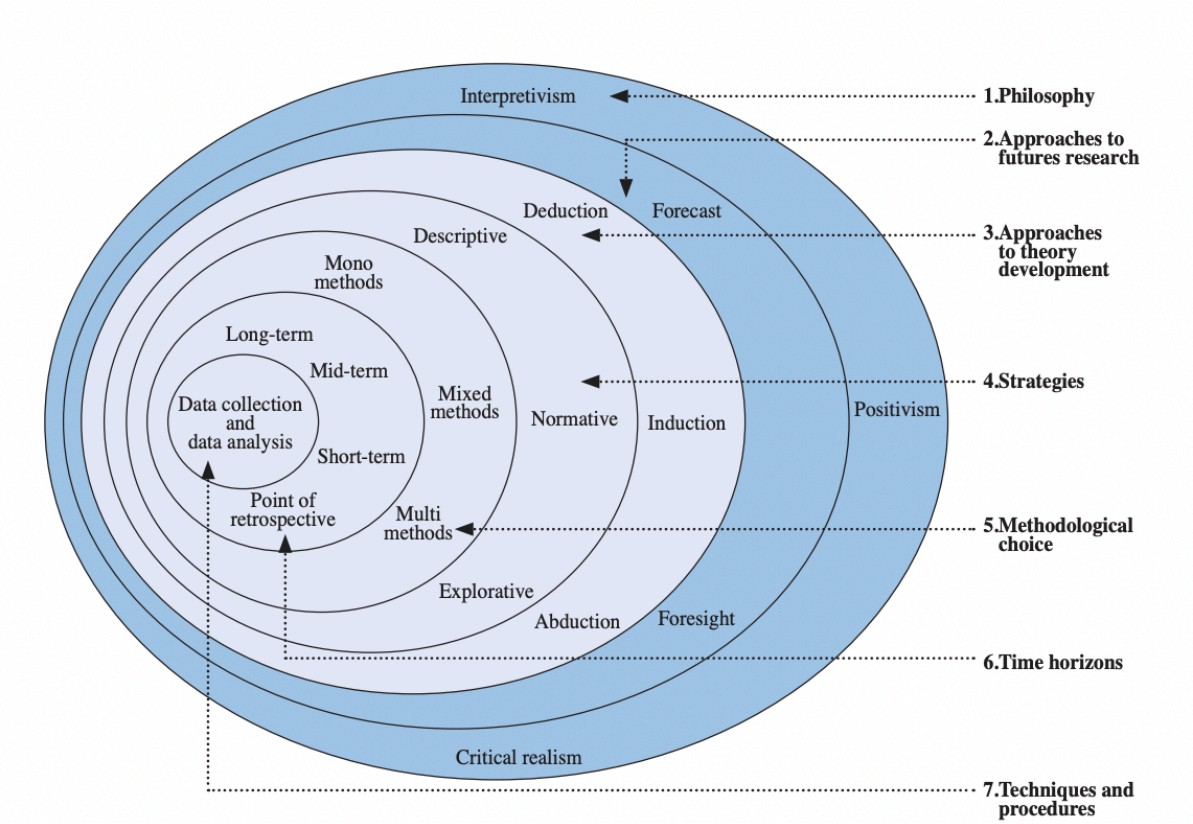

Figure 1: 7-layer research onion framework by Melnikovas (2018)

4.1 Research philosophy (Layer 1)

Undertaking a research project means partaking in the development of new knowledge, and part of this process includes recognizing and acknowledging the researcher's underlying assumptions and philosophical perspective Saunders et al. (2019, p. 130). The establishment of a solid theoretical framework not only forms the basis for the research process, but also determines the way in which findings will be interpreted (ibid). According to Saunders et al. (2019, p. 131), the credibility of a research project is contingent upon the research philosophy. Thus, it is crucial to thoroughly examine the rationale behind the given philosophical standpoint, while ensuring it will underpin the research consistently throughout the process.

Before examining philosophies, there are typically three assumptions to consider. The first assumption is the rather abstract "ontology", which looks at the nature of how we perceive reality. This assumption asserts that the researchers are interested in existential questions such as what and how, and that these questions shape their worldview (Saunders et al. 2019, p. 133). Ontology is often characterized by subjectivity, which potentially might result in a lack of diverse perspectives (Saunders et al. 2019) The second assumption is "epistemology", which looks at what is considered real knowledge. In the field of business and management research, Saunders et al. (2019, p. 133) asserts that several forms of information may be utilized, including but not limited to facts, imagery, perspectives, written content, and stories. Epistemology is often characterized by objectivity, and the absence of complexity and richness tend to be a disadvantage of this assumption Saunders et al. (2019, p. 134). The third assumption is "axiology", which pertains to the impact of personal values on the research process (ibid). More precisely, how one's values influence the preference for qualitative data versus quantitative data, and why one topic was deemed more important than others. Axiology is often characterized by subjectivity because of how the researchers' own values influence the research process (ibid). This can be problematic as the research process will favor one set of values over another, and by that encounter a lack of inclusion of other perspectives in the decision-making process.

As our RQ seeks to answer *how* the digital euro should be designed, the most appropriate standpoint to take is an ontological one. Our primary goal is to assess *what* fosters trust and *how* this should be manifested into the design of the digital euro. Having established our primary underlying assumption, we can now look at the philosophical standpoints. Saunders et al. (2019) suggests there are five different philosophical standpoints: 1) Positivism, 2) Critical realism, 3) Interpretivism, 4) Postmodernism and 5) Pragmatism. Due to the nature of our RQ, this thesis will employ two philosophical standpoints: critical realism and pragmatism.

Critical realism: According to Saunders et al. (2019, p. 147), there are two levels to comprehending the world within the realm of critical realism. The first level pertains to the pure experiences we encounter, and what it is possible to observe from simply experiencing. The second

level pertains to how we process these encounters psychologically and looks at what might have caused us to experience them the way we did. Pure realists believe that the first level is sufficient, whereas critical realists believe that the second step is vital in grasping all of the underlying causes of why we experience the way we do. The central idea of this philosophical perspective is in the recognition that while a subject or problem may only present itself on the surface, it is important to delve into all the underlying reality to see and fully understand the bigger picture. Melnikovas (2018, p. 37) further explains how critical realists accept the premise that several potential realities exist in the future, and the actualization of a given reality will to some extent be shaped by the decisions, contexts and events happening today. This philosophy seems appropriate as a base for answering our research question, as we indeed seek to understand the full picture and underlying mechanisms of trust in the Digitial Euro.

Pragmatism: Adopting a pragmatic philosophy is also appropriate for this thesis, as we seek to directly contribute to real-world problems and decisions. Pragmatism takes theories and looks at their potential to facilitate effective implementation in real-world contexts. The primary goal of adopting this philosophical perspective is to make significant contributions to the progress of knowledge on the respective topic, rather than pursuing the discovery of a single universal truth (Sauders et al. 2019, p.151). Hence, in addition to gaining an understanding of the complete picture and underlying mechanisms of trust in the digital euro, we intend to contribute to the real-world decisions regarding its optimal design.

4.2 Approaches to future research (Layer 2)

According to Melnikovas (2018, p. 38), there are two distinct ways of approaching future research, namely forecast and foresight. Forecasting is mostly known to be quantitative, and based on the assumption that the future can be predicted by analyzing the past. On the contrary, foresight can employ both quantitative and qualitative methods, and tends to be used under the assumption that that several future scenarios exist, and that predicting outcomes is a complex undertaking that extends beyond the examination of the past. Historically forecasting has been the most utilized method, however, while analyzing political, institutional and cultural topics Melnikovas (2018, p.

38) recommends utilizing foresight to get a more comprehensive picture. In this thesis, we will employ the approach of *foresight* to investigate the complex concept of trust alongside the novel development of the digital euro.

4.3 Approaches to theory development (Layer 3)

Once we have established the underlying assumptions, the philosophy and the approach to future research, the subsequent step is to delve into theory development. According to Saunders et al. (2019, p. 152), there are three primary methods for theory development, namely deduction, induction, and abduction. Deduction is utilized to derive specific evidence from broader theories and is founded on the principles of logic. Deduction tends to be quantitative and most of the time pertains to a positivistic philosophy (Saunders et al., 2019, p. 154). Induction on the other hand, seeks to develop theories based on the analysis of empirical data, and is by nature much more explorative. Induction is derived from disciplines within social sciences and has been acknowledged by scholars to aid the process of interpretation and exploration. It is an approach that derives general conclusions from specific observations, by allowing for explanations beyond those initially anticipated. Most often, induction pertains to an interpretivist philosophy (Saunders et al., 2019, p. 155). The last approach is abduction, which is commonly referred to as a hybrid between deduction and induction. The abductive approach typically starts with an observation, followed by the development of a thorough theoretical framework, which is subsequently tested using both existing and novel data. The abductive approach tends to be foundational to pragmatism and critical realism, although it is commonly used in management research due to its versatility. For the purpose of this thesis, we seek to take an abductive approach to answer our RQ.

Secondary data

Secondary data is, according to the definition provided by Saunders et al. (2019 p. 338), data that has previously been gathered to answer a different research objective. Nevertheless, this type of data can be a meaningful source of information and can aid in the overall comprehension of a research topic. In this thesis we will be using an abductive approach and will therefore first be exploring our research objective through a theoretical framework based on previous literature

and theories; thus, secondary data play a crucial role in our methodology. The theoretical framework will be developed using a variety of secondary sources, including reports and journal articles, to get an understanding of how trust has previously been researched in relation to relevant artifacts such as cryptocurrencies and other CBDCs. We seek to derive a theoretical framework from secondary data to see how this might translate to trust in the digital euro. We will explore this through our collection of primary data, which will be discussed later in this section. Saunders et al. (2019 p. 345), notes that one of the main drawbacks of secondary data is its possible inability to transfer directly to another research objective. However, our aim is to use the secondary data sources as a guide to get closer to answering our RQ, while accounting for the possibility that they may not be entirely appropriate and suitable. We describe how we have ensured the reliability and quality of our secondary data in chapter 2 of our literature review.

4.4 Research strategy (Layer 4)

Melnikovas (2018, p. 39) defines research strategy as the process of gathering primary data and lists three different approaches to help guide future studies. The first strategy is *descriptive* and mainly aims to get precise forecasting of future characteristics and attributes. Thus, this strategy is mostly quantitative and utilized in combination with deductive forecasting methods. The second strategy is *exploratory* and examines how future events potentially may unfold. This strategy is more qualitative and inductive in nature, as it seeks to discover several potential future scenarios. The third strategy may be characterized as *normative or prescriptive* and pertains to the aim of influencing future outcomes by identifying the key components or events necessary to achieve a particular objective. For this thesis, it is suitable to utilize the normative/prescriptive strategy, as we seek to identify which attributes the digital euro should have to foster trust once its development is finalized.

4.5 Methodological choice (Layer 5)

This layer pertains to the decision taken on the primary data collection method to answer the research objective. The choice involves the consideration of utilizing either quantitative or qualitative approaches or a combination thereof. When only one approach is utilized, it is

referred to as mono-method. Conversely, when both techniques are utilized, it is referred to as a mixed methods data collection (Melnikovas, 2018, p. 39). In this thesis we will employ a mixed methods approach, utilizing mainly qualitative data and to some extent quantitative data. Qualitative methods will be utilized mainly to obtain a rich and deep understanding of a research question, following critical realism, in which we strive to understand all underlying mechanisms for a phenomenon. Quantitative methods will be utilized to address the findings in a more objective manner, by also quantifying the results. Our rationale behind choosing both methods is underpinned by Ivankova et al. (2009, p. 136), who asserts that mixed methods may be beneficial to use when aiming to broaden the scope of research beyond what is possible from just using one of the methods.

Primary data

To obtain our qualitative data, we utilize the Delphi method. The Delphi method is a systematic qualitative methodology to forecast a particular topic based on the opinions of subject matter experts (Chuenjitwongsa, 2017; Thoring et al., 2022, p. 5799). The Delphi method involves iterative rounds of questions whereby the panelists remain anonymous to one another throughout the duration of the study, and their answers are shared in anonymous form with the rest of the panelists to stimulate reflection so that consensus or forecasting of future scenarios is achieved (Amos et al., 2008; Thoring et al., 2022, p. 5799). Brady (2015) further explains how the Delphi method seeks to contribute practically to decision making and therefore makes it well suited for the pragmatic research philosophy.

To reach consensus on how the digital euro should be designed to foster trust compared to bitcoin, our Delphi method relied on a panel of experts that had subject matter expertise on either or CBDCs, the digital euro, cryptocurrencies and bitcoin. Thus, we identified five experts who were invited and agreed to participate in our Delphi study. See the final list of participants in Table 4. Two panelists (panelist 1 and 2) asked to remain anonymous in our thesis paper, and thus pseudonyms are used. Our Delphi study involved two iterative rounds, the first round being a semi-structured interview and the second round being a survey form (see Chapters 4.6 and 4.7

for further details). The panelists remained anonymous to one other throughout both rounds of the Delphi study in accordance with the Delphi method.

Table 4: Panelists

Name	**Industry**	**Role**
Panelist 1	Blockchain, IT, digitalization	Consultant at a big 4 consulting firm
Panelist 2	Fintech and cryptocurrencies	Lawyer
Sarah Palurovic	Blockchain	Executive Director at the Digital Euro Association
Somnath Mazumdar	Blockchain and computing systems	Assistant Professor at Copenhagen Business School (CBS) in the Department of digitalization
Søren Laurits Nielsen	Bitcoin	CEO of Bitcoin Suisse Denmark

4.6 Time horizons (Layer 6)

Brady (2015) states that it is common for a Delphi study to involve three or more rounds of iteration and data capture. The first stage of a Delphi study typically involves the utilization of a researcher-developed questionnaire, drawing upon existing literature and/or pre-existing knowledge on the given research area. In the second round, also referred to as the feedback round, each expert is afforded the opportunity to provide their opinions on the answers that were obtained in the initial round. The third round involves a questionnaire that draws upon the information gathered in rounds one and two with the objective of attaining a shared consensus on the subject matter. If it is not possible to establish a shared consensus by the third round, it may be necessary to employ more rounds to reach consensus (ibid).

For this thesis we have determined that conducting two rounds of data collection is sufficient in addressing our research question. This has been decided based on the number of panelists and the nature of our RQ. The first round will be a semi-structed interview guided by the theoretical framework established from secondary data, and the second round will be a

survey that draws upon the information gathered in the initial round aiming to reach a shared consensus amongst the panel.

4.7 Techniques and procedures (Layer 7)

Layer 7 of the research onion pertains to figuring out how to optimally utilize the identified approaches across all preceding layers. Thus, the subsequent section will outline how we intend to conduct and analyze our primary data from the Delphi study.

Delphi round 1

Developing the interview guide

As indicated in the preceding section (4.3), our research approach is characterized by abductive reasoning, wherein we do not solely aim to test an existing theory nor solely develop a novel one. To best integrate an abductive line of reasoning into our Delphi study, Thompson (2022, p. 1415) suggests that it is imperative to ensure the themes of the study are guided, rather than predetermined by a theoretical framework. Thus, the first round of our Delphi study will comprise a semi-structured interview, guided by our theoretical framework on trust in digital currencies (see table 5). The interview questions pertain to the five overarching topics outlined in our theoretical framework, specifically: social trust factors, institution-based trust factors, technological trust factors, economic (hard) trust factors and socio-technical (soft) trust factors while also allowing for questions and discussions beyond these thematic concepts to foster a more exploratory and interpretive interview. This allows us to address the main RQ by seeking to identify the trust factors that are most relevant for the design of the digital euro to foster trust. The interview guide was developed deductively based on our theoretical framework (Table 5). Nonetheless, we simultaneously allow for abduction during our interview by keeping the format semi-structured and throughout our data analysis to allow for the exploration of new ideas that have not been identified within the existing body of theory or literature.

Moreover, the interview questions were thoroughly crafted with due regard to the risks associated with trust in bitcoin, as identified in our literature review. These risk factors are

denoted by a minus symbol (-) in our theoretical framework (refer to table 5). By incorporating questions that directly addressed the extent to which these risks would be countered or mitigated in the design of the digital euro, we ensure that we effectively answer the sub-RQ 2 and part of the main RQ pertaining to the comparison with bitcoin.

Analyzing the results

After completing the interviews with all five panelists, we utilized the software tool NVivo to code the collected data. We employed a coding strategy drawing upon the approach outlined in Fletcher and Marchildon's (2014) abductive Delphi study, where they combined both deductive and inductive methods to code their interviews. Guided by this, we first establish a codebook of pre-determined codes, derived from our theoretical framework stemming from the most up-to-date literature on trust features in digital currencies (see table 5). The predetermined codes of the codebook reflect the deductive aspect of our research approach. In this process, any statements from the interviewees that relate to the predefined code themes were systematically coded in alignment with these codes. Secondly, responses that deviate from the predetermined codes are categorized as 'others'. Subsequently, these are coded based on their thematic content. This reflects our inductive approach, fostering an explorative coding process. This inductive approach to coding allows us to expand the initial theoretical framework by a total of five codes, namely, cultural differences, communication, user experience, sustainability and inclusivity.

Furthermore, we ensured intercoder reliability by having both authors of this present thesis independently code the transcripts. Thereafter we cross-referenced our coding results to evaluate the consensus and divergence in the codes assigned to responses within the same unit of text. This process aimed to eliminate the influence of personal biases and to ensure the reproducibility of the coding process by other knowledgeable coders.

Once the coding of the interviews had been completed, we began analyzing the findings. We first set out to determine the consensus and non-consensus issues in the interview responses (Chuenjitwongsa, 2017). For the purposes of this thesis, we decided that consensus is reached on

issues that have reached agreement among four or more panelists ('consensus issues'). Issues that were only agreed on by less than four panelists were considered issues that did not reach consensus ('non-consensus issues'). Following the Delphi process guide by Chuenjitwongsa (2017), these non-consensus issues were included in a survey for the second Delphi round to establish final consensus on these issues (see figure 2). Findings of both consensus and non-consensus issues from the first Delphi round are reported and analyzed in relation to findings from our systematic literature review. In our findings chapter, we analye the findings that we consider most noteworthy and significant in answering our RQ and sub-RQ 2, as well as for designing the second round of our Delphi study.

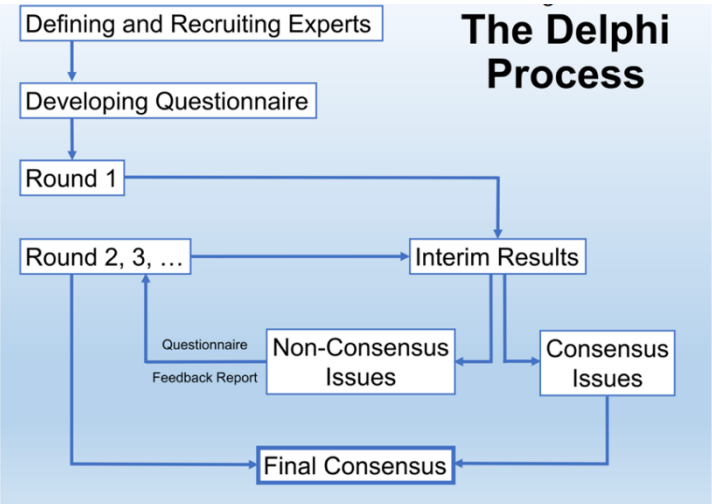

Figure 2: The Delphi process by Chuenjitwongsa (2017)

Delphi round 2

The second survey was developed with the aim of reaching consensus on non-consensus issues derived from the interview of the first Delphi round. There was a total of 34 non-consensus issues identified from the first Delphi round. Due to time constraints and to maintain

the response rate among our panelists for the second Delphi round, we decided to select non-consensus issues that were most relevant to answering the main RQ.

Thus, out of 34 non-consensus issues, we decided to exclude those that pertained to external trust factors and move forward with the internal trust factors for the second Delphi round. This decision was made as our main RQ asks how the ECB should design the digital euro. Arriving at a consensus on internal factors which the ECB have direct control and influence over would help us to directly address the main RQ and better advice the ECB on the trust factors that the panelists deem must be important in considering for designing a trustworthy digital euro. External trust factors were included in the first Delphi round to understand the dispositional and environmental factors that could influence trust in the digital euro, however these factors are not something that the ECB has direct control or influence over, which is why we decided to exclude them from the second Delphi round. Although we did not reach clear consensus on external trust factors, these factors are nevertheless still significant to our research. As we will elaborate later in the analysis and discussion chapters, these factors serve as valuable indicators for the ECB to take into account, allowing us to provide more informed recommendations for the design of the digital euro.

Furthermore, we decided to omit non-consensus issues or questions pertaining to bitcoin during the second Delphi round. The reason is twofold. Firstly, we observed that several of our panelists faced challenges in understanding or aligning with the research motivation to compare the digital euro and bitcoin. The panelists expressed that the two are distinct assets serving different uses cases, making it challenging to draw concise comparisons when asked about bitcoin-related questions. Secondly, as previously mentioned, we were required to prioritize non-consensus issues that would best guide our recommendations to the ECB regarding the features that are crucial to consider in the digital euro for establishing trust.

Developing the survey

The survey comprised of two questions. The first question asked panelists to rank 13 technological and economic trust factors that did not previously reach consensus on a rating scale from 'most important' (1) to 'least important' (13). We provided an overview of the trust features that had already attained consensus in the first round to ensure that the panelists were aware of what was previously agreed upon. The second question in the survey asked panelists to explain their rationale behind their choice of ranking. This allowed us to collect both quantitative and qualitative answers.

Arriving at a strong and clear consensus amongst all panelists is nearly impossible due to the high degree of uncertainty and heterogeneity of the panel that tend to foster diverging opinions (Woudenberg, 1991). Keeping this limitation of the Delphi study in mind, we decided to collect qualitative comments since literature on Delphi studies have argued that exploring the different arguments behind why the panelists disagree yields greater insights than assessing predictions where consensus can easily be achieved (Gordon and Pease, 2006; Story et al., 2001). Furthermore, having only two questions in the survey helped to mitigate the risk of overwhelming our panelists with the time and effort required for survey completion. By keeping the survey short and concise, we were able to attain a 100 percent response rate from all our panelists.

Furthermore, preserving the anonymity of panelists' responses is a fundamental principle in a Delphi study. As such, we refrained from disclosing any information about the identities of panelists or the responses and opinions they had previously expressed regarding these non-consensus issues.

Analyzing the result

After obtaining the survey data from all five panelists, we will proceed to perform a Kendall's W coefficient of concordance. This method is suggested by Paré, G et al. (2013, p. 212) as appropriate when analyzing qualitative Delphi data involving rankings. Kendall's W is typically applied in the context of comparing several rankings (Bar-Ilan, J. 2005), as it provides an overall assessment of the consensus level amongst multiple submitted responses. Thus, pertinent for our

analysis with a panel comprising 5 experts. Paré et al., (2013, p. 212) presents various Kendall W values and indicate that $W > 0.7$ serves as a suitable threshold to conclude a strong degree of consensus, which will serve as the guide for our analysis. Paré et al., (2013, p. 212) further suggests analyzing the mean scores, while also considering the factors that fall within the top and bottom ranges of the ranking. This will be included in the analysis as well. Lastly, we will look at the variance on the individual mean scores, to get closer to understanding the consensus level on each individual factor.

4.8 Quality evaluation

Landeta (2006) lists several factors that can increase the overall quality of a Delphi study, namely quality of the selected panel, duration of time between rounds, and quality of the answers. These factors will be used to assess the quality of the present research and the chosen Delphi method.

Firstly, the quality of the panel was accounted for by selecting experts from a broad range of industries. As Millar et al. (2007) notes, it is vital to have a panel encompassing multiple backgrounds and diverse perspectives. We ensured to have panel with both legal, technological, academic, and business-oriented expertise. Hasson (2000, p. 1013) supports this claim by arguing that the content validity of a Delphi study improves where participants exhibit a greater amount of knowledge regarding the subject matter. Landeta, J. (2006, p. 469) additionally lists attrition rate to be of uttermost importance when evaluating the quality of a panel in a Delphi study, which we successfully managed to achieve, by carrying over all five panelists from the first to the second round.

Next, Landeta (2006) asserts that the timeframe of a Delphi study plays an important role in determining its quality. Nevertheless, there is a lack of existing literature providing a clear definition of what an ideal timeline for a Delphi Study looks like. However, Varndell et al. (2021, pp. 7) argues that in terms of timeline assessment, shorter timeframes tend to promote more valid results and better retention. We therefore kept the time between round 1 and round 2 as short as

possible, more specifically; about one week. By doing so, we sought to limit the risk of participants dropping out, changing their initial outlook or becoming biased from external sources.

Lastly, Landeta (2006) describes the quality of the answers as a reflection of the study's overall quality, while indicating that rich and extensive answers equal high quality. We took two steps to ensure maximum quality of the panelist's responses. In round one we opted for a semi-structured interview guide allowing participants to provide comprehensive, in-depth and additional answers to our questions. Further, we had initially allocated 45 minutes for the interviews, allowing the participants to go overtime if they wished to share additional thoughts or comments beyond the standard interview questions. This approach was designed to accommodate for any additional responses that could enhance the overall quality of their answers. In round 2, we asked the panelists to explain their rationale for their choice of ranking at the end of the survey to ensure a comprehensive data collection process.

4.9 Ethical considerations

Saunders et al. (2019 p. 253) asserts that the ethical considerations shaping a research project pertain to how the individuals of investigations are impacted by the process. To effectively address possible ethical dilemmas in our Delphi study, we have undertaken a number of measures.

Firstly, Hasson (2000), lists anonymity as an ethical factor researchers should be aware of when conducting a Delphi study. This is because the method is distinctively known for being anonymous, which fosters an environment with minimal bias and reduced pressure to answer a certain way (ibid). We preserved anonymity throughout each of the Delphi rounds, by ensuring no information about any participant was shared to the panel. Yet, Hasson (2000) explains that for a Delphi study to be considered fully anonymous, the participants must remain so even to the researcher, and if that is not the case, it is more appropriate to consider the Delphi study “quasi-anonyme”. Given our responsibilities for conducting the study, which involved responsibilities such as participant recruitment, conducting interviews, and following up on responses, we were able maintain only a quasi-anonymous study. This could potentially jeopardize the initial rationale

for ensuring complete anonymity in a Delphi study, more specifically the risks of bias and pressure. However, we expect this to have minimal impact on the study. It would be evident to the experts that we as student researchers lack both authority and expert knowledge necessary to induce these risks.

We further contacted each participant individually with a consent form, stating that their data would be processed in line with General Data Protection Regulation (GDPR). While also asking them about their willingness to disclose name and institutional information in the final report. In cases where participants asked to remain anonymous, we pledged to do so by referring to them in this thesis using pseudonyms. Lastly, we ensured verbal consent from all participants before transcribing their interviews.

5. Theoretical Framework

To answer the main RQ of the present thesis on the trust factors that ECB should consider in designing the Digital Euro, we must first address sub-RQ 1: *How and what mechanisms establish trust in digital currencies?* To answer this question, a theoretical framework is needed to help us understand the concept of trust and its relationship to digital currencies, specifically the Digital Euro and Bitcoin. As we seek to employ a deductive approach to answer the main RQ of this thesis, establishing a theoretical framework will serve as a guide to determine the trust factors that are relevant to the Digital Euro in comparison to bitcoin.

We begin by presenting the Cryptocurrency Trust Model developed by Elsokkary et al. (2022), which offers a comprehensive framework detailing the key trust factors that are deemed necessary for designing a trustworthy cryptocurrency. The components of the Cryptocurrency Trust Model are described in detail, along with an analysis of their limitations based on the findings from our earlier literature review. To address the limitations of the Cryptocurrency Trust Model and expand the framework's applicability to non-cryptocurrencies namely the Digital Euro, we incorporate theories on institution-based trust by McKnight et al. (2002) and economic and social

trust factors of currencies proposed by Wonneberger and Miel (2012). Lastly, the trust factors that will be evaluated in our interview with industry experts are presented in table 5. The trust factors listed in table 5 will guide the design of interview questions to assess the relevancy and importance of these trust factors in the context of the Digital Euro, which will answer the main RQ of the present thesis.

5.1 Cryptocurrency Trust Model

Elsokkary et al.'s (2022, p. 76) Cryptocurrency Trust Model is illustrated in figure 3. The model builds upon the TrUStAPIS model by Ferraris and Fernandez-Gago (2019, p. 111). The TrUStAPIS model provides a framework for ensuring trust in Internet of Things (IoT) systems throughout their software development lifecycle, focusing on seven essential requirements: Availability, Usability, Privacy, Trust, Security, Identity, and Safety (Ferraris & Fernandez-Gago, 2019, p. 113). These requirements are grounded in requirements engineering in software development engineering, which is the first phase undertaken in software development that involves developers to gather requirements based on stakeholder needs (Ferraris and Fernandez-Gago, 2019, p. 111). Ferraris and Fernandez-Gago (2019) assert that the seven essential requirements identified above are requirements that any IoT system needs to elicit to guarantee and increase trust in an IoT entity.

According to Elsokkary et al. (2022, p. 73) the significant similarities between IoT and blockchain, including its overall distribution and decentralization, allow for the applicability of the TrUStAPIS model in cryptocurrency trust modelling. Elsokkary et al. (2022) expand upon the seven trust requirements outlined by the TrUStAPIS model to include trust requirements unique to blockchain technology, as well as social and dispositional trust factors. These requirements are identified through previous research findings and through their own analysis of specific trust requirements identified through a case comparison of Bitcoin and Diem, the latter being a cryptocurrency developed by Meta Platforms, Inc. Similar to the TrUStAPIS model, the

goal of the Cryptocurrency Trust Model is to steer cryptocurrency development towards creating currencies that promote increased levels of trust (Elsokkary et al., 2022, p. 73).

The Cryptocurrency Trust Model considers both internal and external trust factors that influence overall trust in cryptocurrencies. Internal trust factors are grounded in requirements engineering and are technical characteristics that are intrinsic to cryptocurrencies (ibid). There are eight overarching internal trust factors identified in the model: performance, portability, usability, dependability, identity, security, privacy and decentralization (Elsokkary et al., 2022, p. 76). As these are technical features intrinsic to the cryptocurrency in question, developers have control over the influence of enhancing these features to increase user trust (Elsokkary et al., 2022, p. 74). The authors note that each of the eight characteristics can be linked to other factors at the same time. Additionally, the authors have identified several sub-characteristics that fall under each of the eight overarching trust factors, which will be detailed later in this chapter. External trust factors are non-technical and dispositional factors affecting trust in cryptocurrencies and therefore are beyond the control of developers of cryptocurrencies (Elsokkary et al., 2022, p.76). The authors note that external trust factors may yield greater influence over trust in cryptocurrencies than internal trust factors (ibid). The solid arrows represent requirement types, the dotted arrows represent the relationship between the requirements, and the arrows represent the contribution of requirement type to overall trust (ibid).

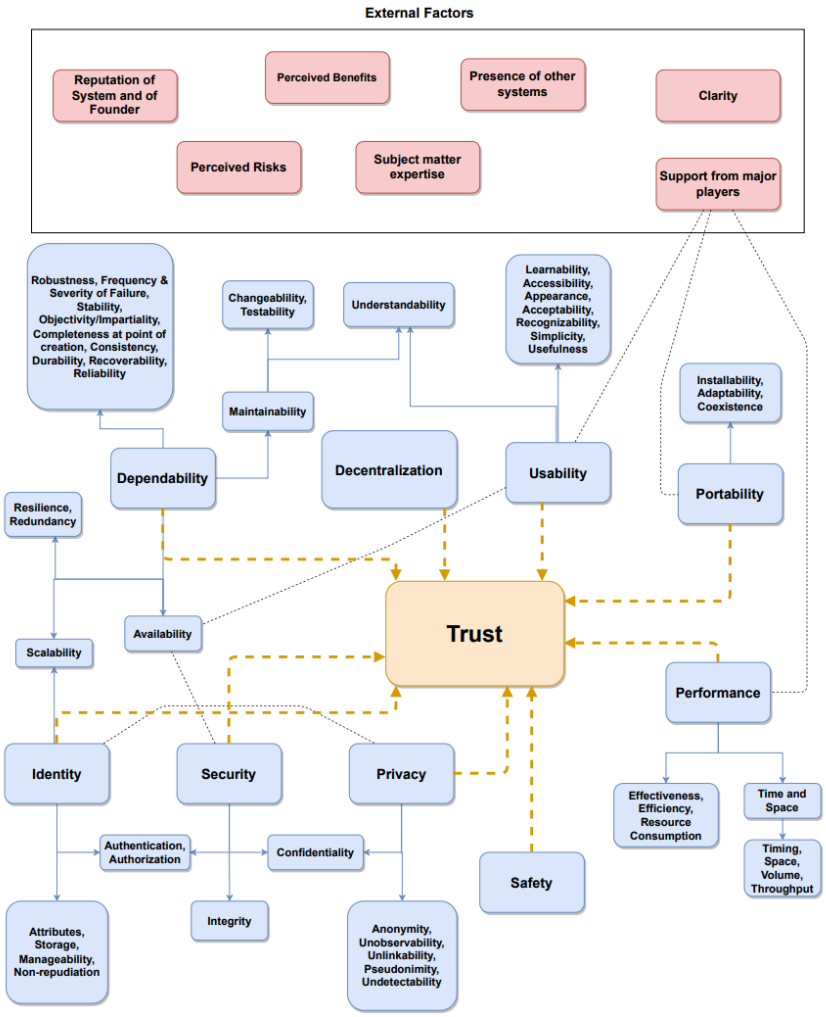

Figure 3: Cryptocurrency Trust Model by Elsokkary et al. (2022)

Definitions and remarks for each of the seven external trust factors and eight internal trust factors identified in the model are provided below. Although concrete definitions for each trust factor are not explicitly provided by the authors, an interpretation of what the authors mean by these seven external trust factors will serve as definitions for each trust factor.

External trust factors in cryptocurrencies

1) The presence of other systems

This trust factor is inspired by Craggs and Rashid's (2019) work on trust in blockchain systems. Craggs and Rashid (2019, p.22) argue that Bitcoin is not totally trustless as there are other systems in the Bitcoin and cryptocurrency ecosystem that are essential to securing trust. The ecosystem relies on people, including developers, miners and validators for its implementation and continuous operation. Thus, although Bitcoin was designed with the aim of fully mitigating risks associated with human behavior, there have been instances of both intentional and unintentional harmful actions within the Bitcoin network.

2) Perceived risks

This factor can be influenced by various factors, such as the absence of clear regulatory guidelines, involvement in illegal activities, and the absence of incentive structures (Elsokkary et al., 2022, p. 75). The lack of well-defined regulations applicable to cryptocurrencies raises concerns among both regulators and potential users regarding liability in the event of cyberattacks or hacks (ibid). The presence of illegal activities such as terrorism financing and money laundering made possible by decentralized and anonymous transactions can also contribute to the perceived risk associated with using cryptocurrencies (ibid). According to Albayati and Rho (2020, p. 9), trust and risks have an inverse relationship whereby an increase in trust leads to reduction in expected risks. The authors argue that trust plays a mediating role in increasing users' belief in a new technology (ibid).

3) Perceived benefits

This factor alludes to whether the average person can perceive the benefits of using cryptocurrencies over traditional fiat currencies (Elsokkary et al., 2022, p. 74). For example, the degree to which the average person will perceive of the benefits of using cryptocurrencies is explained by the authors as being context-dependent, as individuals living in industrialized countries where financial systems are trusted and carried out quickly, these perceived benefits

may outweigh those of cryptocurrencies (ibid). On the other hand, people living in countries where the local currency is volatile to which cryptocurrencies may be more trustworthy form of asset and transaction (ibid). In Gupta et al.'s (2023) study, perceived benefits and perceived risks of the digital rupee were both found to have an impact on trust; hence, these warrants both factors to be included in our theoretical framework to assess their importance in the context of the digital euro.

4) Subject matter expertise

This external trust factor is derived from a previous study conducted by Khalifa et al. (2019, p. 311) that examined the trust aspects within blockchain systems. The authors theorize that trust in blockchain technology is related to trust in online transactions, which is guided by background, knowledge, prejudices, and experience (ibid). If these are lacking, users will likely stick to traditional ways of transacting (ibid). The same logic is applied to blockchain technology, where without prior user knowledge or experience with the technology, users will not be able to trust the technology simply on the basis that the technology should be trusted cryptography rather than fallible humans or institutions (ibid). Hence, the authors argue that other characteristics exhibited by blockchain technology are needed to be able to foster trust among users who possess minimal knowledge of how the technology behind blockchain works (ibid).

5) Reputation

According to Elsokkary et al. (2019, p. 74), the reputation of a cryptocurrency's founder can significantly influence user trust in the currency. The authors demonstrate this by examining the impact of the founder's reputation on users' perception and trust in Diem and Bitcoin (ibid). Centralized cryptocurrencies like Diem have been associated with Facebook and its controversial mishandling of user data (ibid). In contrast, Bitcoin was introduced by an anonymous entity named Satoshi Nakamoto, ensuring that it remained free from any negative reputation or human influence (ibid). While developers have limited control over reputation, it is important to

consider reputation when evaluating the trustworthiness of centralized cryptocurrencies that are closely associated with human creators (ibid).

6) Clarity

Clarity is an external trust factor that pertains to the degree of transparency, precision and comprehensiveness in the regulatory framework and the promises made by cryptocurrencies (Elsokkary et al., 2022, p. 75). The absence of explicitness in regulations surrounding cryptocurrencies has generated doubt regarding accountability, repercussions in case of cyber-attacks, strategies to handle hacking incidents, and harmonization of financial norms across various nations (ibid). Thus, greater clarity on policies and promises can enhance public trust in cryptocurrencies (ibid).

7) Support from major players

The involvement and support of institutional players can significantly shape trust in the cryptocurrency space. ace. The existing trust that users have in institutional players reinforces the trust users have in cryptocurrencies, reassuring them of the value of the project. Elsokkary et al. (2022, p.74) point to anecdotal evidence that underscores the significant influence corporations can exert on overall user trust in the cryptocurrency ecosystem. For instance, the value of major cryptocurrencies rose following Facebook's announcement of the Diem project (Bouoiyour & Selmi, 2019). In contrast, trust significantly decreased when several influential corporations like PayPal, VISA, MasterCard and eBay pulled out of the Diem project (U.S House Committee on Financial Services, 2019). Institutional support can also be important for building user trust, as it facilitates the technical integration of centralized and decentralized financial ecosystem that allows for greater usability and portability of cryptocurrencies (Elsokkary et al., 2022, p.74).

Internal trust factors in cryptocurrencies

1) Performance

Performance is defined as how well the trustee performs a task (Hoff & Bashir, 2015, p. 424). The quality of performance of an automated system has been found to be strongly correlated to the level of trust (ibid). Elsokkary et al. (2019, p. 76) include the following sub-features: Effectiveness, Efficiency, Resource Consumption, Time and Space (Timing, Space, Volume, Throughput)

2) **Portability**

This feature refers to the quality of the design of the system (Chung & Leite, 2009, p. 368). The portability attributes of cryptocurrencies include Installability, Adaptability, Coexistence (Elsokkary et al., 2020, p. 76).

3) **Usability**

Usability is defined as the ability of a product to be understood, learned, operated and appealing to users as they strive to accomplish specific goals with both effectiveness and efficiency in particular contexts (Baharuddinet al., 2013, p. 2225) . Elsokkary et al. (2022, p. 76) identifies the following sub-features of usability: Learnability, Understandability, Accessibility, Appearance, Acceptability, Recognizability, Simplicity, Usefulness

4) **Dependability**

Dependability refers to the ability of a system to deliver services that users can trust (Avizienis et al., 2004, p. 13). In other words, the concept pertains to a system's ability to prevent performance failures that exceed acceptable thresholds in terms of both frequency and severity (ibid). According to Elsokkary et al. (2022, p. 76), attributes of dependability encompass the following: Maintainability of the Code (Understandability, Changeability, Testability), Robustness, Frequency and Severity of Failure, Stability, Objectivity or Impartiality, Completeness at Point of Creation, Consistency, Durability, Recoverability, Reliability, Availability (Resilience, Redundancy, Scalability).

5) **Identity**

According to Ferraris and Fernandez-Gago (2019, p. 117) knowing the entity with which a system interacts is an antecedent to trust. The system must be able to authenticate and authorize the interacting entity based on their identity. However, the authors are careful to underscore that identity is closely correlated with privacy. If the interacting system (e.g., IoT or in this case, a the ECB behind the digital euro) has too much information about the trustor's identity, this can lead to reduced privacy. The following attributes of identity are provided by Elsokkary et al. (2022, p. 76) in the context of cryptocurrencies: Authentication, Authorization, Attributes, Storage, Manageability, Non-repudiation, Scalability.

6) **Security**

Security in cryptocurrencies can be enhanced by ensuring the following security characteristics are properly in place: Authentication, Authorization, Integrity, Confidentiality (Ferraris and Fernandez-Gago, 2019, p. 116; Elsokkary et al., 2022, p. 76).

7) **Privacy**

The following attributes of privacy can ensure that the system (trustee) not only upholds and ensures the privacy of users but ensures that personal data, if used by the vendor for commercial purposes, does not risk leaking sensitive personal information that may damage users' trust in the vendor (Ferraris and Fernandez-Gago, 2019, p. 117). Privacy attributes include Confidentiality, Anonymity, Unobservability, Unlinkability, Pseudonymity, Undetectability (Elsokkary et al., 2022, p. 76).

8) **Decentralization**

Elsokkary et al.'s (2022, p. 76) identify decentralization as a technical feature yielding strong influence on trust in cryptocurrencies. The increase in decentralization of cryptocurrency was correlated with greater trust as it decreases or entirely removes the influence of external factors that would otherwise yield a greater influence on trust in cryptocurrencies than internal trust features (ibid).

5.2 Limitations of the Cryptocurrency Trust Model

The Cryptocurrency Trust Model by Elsokkary et al. (2019) serves as a comprehensive model to guide developers in designing cryptocurrencies to ensure trust. However, we identify two significant limitations that impede the model's direct applicability in addressing both our sub-RQ1 and the main research question. Firstly, the model predominantly focuses on technical aspects such as internal trust factors, neglecting economic characteristics that play a vital role in establishing trust in currencies, such as liquidity, fungibility and stability of a currency. Elsokkary et al. (2019) mention liquidity as a trust-related issue within cryptocurrencies, but they ultimately conclude that it's challenging to classify within the model due to its dual nature as an internal trust factor and a policy-driven factor. This may be appropriate if the trustee being studied is a cryptocurrency as the case for Diem and Bitcoin in which these economic factors have limited relevance. However, in our study, we examine trust in the Digital Euro, a non-DLT-based digital currency issued by a central bank, in comparison to Bitcoin. The Digital Euro is a "currency" rather than a "cryptocurrency," and therefore, it is imperative to incorporate economic trust factors that are characteristic of traditional currencies. This adaptation of the model is essential to effectively address our sub-RQ1 and the overarching research question.

Secondly, the model lacks an explicit mention of institution-based trust factors in the context of cryptocurrencies. While the model does touch upon factors like clarity of policies and support from major players, indirectly alludes to institutional trust factor as defined by McKnight et al. (2002), it falls short of providing a comprehensive understanding of the multifaceted nature of institutional trust. To delve deeper into institutional trust within the cryptocurrency realm, we must consider more than just the clarity of policies and support from major entities. It's essential to also examine the regulatory framework in place to promote trust in the cryptocurrency ecosystem. In essence, regulatory clarity and major player endorsement represent only two facets of institutional trust, leaving a broader spectrum unaddressed. The following section will theorize economic trust factors and institutional trust factors in greater detail, which serves as additional

trust factors to build upon the cryptocurrency trust model in order to effectively address our main RQ and sub-RQ 1 and 3.

5.3 Economic and social trust factors in currencies

The following trust-related functional aspects of currencies are taken from previous works of Wonnegerber and Mieg (2012). Based on a scientific literature review on money and currency systems, the authors have derived hard, soft and idealistic trust factors in money (Wonneberger & Miel, 2012, p. 233). These factors were validated against the Euro, Gold, and German community currencies through a questionnaire using trust-related scales (Wonneberger & Miel, 2012, p. 234). The authors define hard trust factors as related to economic characteristics that foster trust in currencies, including the liquidity, fungibility and stability of a given currency (p.233). Soft trust factors are non-quantifiable characteristics that are characteristic of social or technical systems: backing, credibility, system security, image and manageability (ibid). Idealistic trust factors are characteristic of what the authors call community currencies, which we have also excluded for the purpose of our study as it does not pertain to either the Digital Euro or Bitcoin (ibid). Definitions and remarks for both economic (hard) trust factors and soft trust factors in currencies, as postulated by the authors, are provided below. Nevertheless, given the authors' relatively concise definitions, we offer a more comprehensive elucidation.

Liquidity (hard / economic trust factor)

According to Wonnegerber and Mieg (2012), liquidity pertains to the certainty of a given currency being accepted within a specific region. In other words, they allude a trustworthy currency should be acknowledged as a “medium of exchange” and be accepted as “legal tender”. Knittel, Pitts, and Wash (2019) provide a definition of "Medium of exchange" the facilitation and ease of conducting financial transactions, by having a generally accepted currency. In modern society this is facilitated by currencies, such as Euros, Dollars, Kroners, and Pounds. Further, “legal tender” is referred to by Stiefmüller (2023) as a type of currency with governmental backing that must be accepted as a form of payment to settle both debts and conduct purchases. It

seems appropriate to say that “Liquidity” can be seen as an umbrella term for “Medium of exchange” and “Legal tender”.

Fungibility (hard / economic trust factor)

Fungibility is explained by Wonnegerber and Mieg (2012), as a currency that is suitable for all kinds of financial conducts. Whether it pertains to investments, general purchases or the very act of holding it as an asset. This is similar to the term “"unit of account" explained by Knittel et al. (2019), as the acceptance of a currency being a universal and measurable tool when expressing value. Having one single and widely acknowledged unit of accounts makes it easier to allow for a consistent value comparison and assessment.

Stability (hard / economic trust factor)

According to Wonneberger and Miel (2012), stability of a currency is contingent upon four conditions. 1) The very nature of the currency should be stable, in the sense that it won't be subject to a high degree of volatility and thus fluctuates in value from day to day. 2) The currency should follow the typical trend of inflation and change value according to that trajectory. 3) The currency's value should be stable, meaning it will not devalue over time. 4) The value of any unused currency should remain stable in value, for the purchase of goods and services of equivalent value in a region. Only subject to price variations adhering to the previous three conditions.

Backing (soft trust factor)

According to Wonneberger and Miel (2012), backing pertains to a currency that holds value due to its backing of another asset. Historically, prior to 1971, all circulating currencies were backed by a corresponding amount of gold physically held in the reserves of a central bank, this is also known as the "gold standard". Today, the “gold standard” has become obsolete, and has been replaced by fiat currencies where no physical gold is representing the money circulating. Instead, it is the central bank's job to authorize how much money to print to avoid, for instance, inflation. Thus, the backing of currencies has moved from gold – to the government (central bank).

Credibility of the issuer (soft trust factor)

Credibility is defined by the authors as the credibility of the state and the banks. This is closely related to institution-based trust factors which will be detailed in a later section of this chapter, which pertains to dispositional trust in institutions. Wonneberger and Mieg (2012) argue that both backing and credibility are considered soft trust factors as modern currencies derive their trust from faith placed in the government and the faith of its entire citizenry.

System security (soft trust factor)

System security pertains to the level of protection that a currency provides against forgery and economic crises. Security is one of the eight internal trust factors identified in the Cryptocurrency Trust Model; however, Wonneberger and Mieg's (2012) conceptualization of system security extends beyond security as a mere technical issue by encompassing economic security of currencies. System security is also characterized as an aspect of modern currency that derives its value from administrative rules and policies rather than from its materialistic features like gold.

Image (soft trust factor)

Image is related to the emotional attitude that exists towards a currency. The authors refer to a study by Tyszka and Przybyszewski (2006) which found that the emotional attachment towards the US dollar amongst Polish citizens contributed to an increase in price evaluations by contributing an emotionally driven worth to the currency, augmenting its purchasing value. We argue that this factor is closely related to a sub-feature of institution-based trust, namely digital currency reputation, which will be detailed later on in this chapter.

Manageability (soft trust factor)

Manageability refers to the currency's ability to offer low transaction costs. This factor can be considered a more technical feature in the context of digital currencies and supplements the internal trust factors of the cryptocurrency trust model. It should be noted that manageability was

found to be a hard (economic) trust factor in the Euro whilst it was found to be a soft trust factor in gold in Wonneberger and Mieg's (2012) study.

5.4 Institution-based trust factors

Institution-based trust factors are originally derived from the Web Trust Model by McKnight et al. (2002) which offers insights into the formation and development of trust in the context of e-commerce. Institution-based trust describes the structural characteristics of the environment (the Internet) such as security which can influence a users' level of trust in web-based vendors. The authors define institutional trust factors in two dimensions: structural assurance and situational normality. Structural assurance refers to the belief that legal structures are in place to sufficiently protect against risk. Situational normality is the belief that the environment in which web-vendors operate demonstrates competence, benevolence, and integrity, which the authors argue ultimately determines trusting beliefs and trusting intentions of the web vendor. These definitions are shown below.

McKnight et al.'s (2002) theory on institution-based trust is rooted in Theory of Reasoned Action (TRA) by Fishbein and Ajzen (1975), which contends that beliefs lead to behavioural intentions, which lead to engaging in actual behaviour. This theory aims to predict all forms of human behaviour and has been applied across various fields. McKnight et al. (2011) have extended this theory to account for institution-based trust in the context of e-commerce. Thus, following the TRA, a person's pre-existing belief about the trustworthiness of institutional factors will lead to the intention to engage in a certain behaviour, which will lead to engaging in the actual behaviour.

The relevance of institution-based trust factors in the context of the Digital Euro and Bitcoin has been demonstrated in more recent works. For instance, Tronnier et al.'s (2021) investigation on user intention to adopt the Digital Euro found that pre-existing trust in the ECB has a positive effect on the trust in the Digital Euro. Bijlsma et al. (2021) found pre-existing trust in central banks to have a positive influence on the adoption intention of CBDC. With regard to

cryptocurrencies, Zarifis et al. (2014, 2015) have expanded upon McKnight et al.'s (2002) institution-based trust factors to study trust in digital and virtual currencies. They argue that trust components inherent in e-commerce are the same as those of digital currencies except for institution-based trust factors. For example, they explain that while institutions like VISA, MasterCard, and Western Union dominate the intermediary landscape in traditional transactions in e-commerce, cryptocurrency transactions alternatively depend on other institutional systems like digital wallets and a third-party payment platform for cryptocurrencies like BitPay, which are subject to different regulation or even self-regulated (Zarifis et al., 2014, p. 246). Below are sub-constructs of both situational normality and structural assurance specific to digital currencies that Zarifis et al. (2014 p. 248-9) have validated through qualitative interviews.

1. **Situational normality:** the perception of an environment aligning with expectations and promoting favourable results.
    a. **General structural normality:** prevailing conditions on the internet concerning security and the extent to which they align with expectations.
    b. **Competence (functionality)**: refers to the trustee's capability to fulfil the trustor's needs (McKnight et al., 2002, 337). We parenthesize functionality, as according to McKnight et al. (2011, p. 12:5), competence is a human trust factor whilst functionality is a more appropriate measure of competence in the context of trust in technology, which refers to whether the technology ensures the functionality by supplying the required feature sets essential for task completion, thus delivering as promised.
    c. **Benevolence (helpfulness)**: refers to the trustee acting in the trustor's best interest. In terms of trust in technology, benevolence would be equivalent to helpfulness of a technology offers a help function to complete a task in the absence of a human agent (McKnight et al., 2011, p.12:5).
    d. **Integrity (reliability)**: trustee is committed to honesty and promise keeping. In the context of trust in technology, this would refer to the reliability of the

technology, which is to perform consistently and predictably so that users can trust that the technology will reliably deliver the expected outcome (McKnight et al., 2011, p.12:5-12:6).

e. **Digital currency adoption**: degree to which digital currencies are used and adopted can influence individual behaviour. This is rooted in diffusion of innovation theory by Rogers (1962), which says that consumers with different characteristics will adopt a new innovation depending on the degree and stage of adoption of that innovation.

f. **Digital currency reputation:** person's perception of the reputation of the digital currency can be influenced by media reports, word of mouth, the value of the digital currency in relation to other currencies, security, company success and failures and regulatory developments.

2. **Structural assurance:** the state of and degree to which regulation, laws and guarantees sufficiently protect users against potential risks.
    a. **Digital currency (DC)**: the non-technical characteristics of the currency.
    b. **Government backed currency:** digital currencies and government backed currencies have different structural assurances, and thus trust in former is impacted by the latter.
    c. **DC payment system:** the payment infrastructure of the DC, which is context dependent based on the type of DC.
    d. **Payment intermediary:** refers to the payment intermediary which can facilitate payment transactions of traditional currencies but also embody a reputable third party reinforcing consumer trust in engaging in transactions.
    e. **DC P2P infrastructure:** the peer-to-peer infrastructure of DC which operates differently to traditional currencies and can therefore impact trust on users differently.
    f. **Self-imposed regulation:** the self-governing nature of digital currencies.

g. **External regulation:** state laws, regulations and policies that typically govern traditional currencies.

The sub-constructs of structural assurance by Zarifis et al. (2014, 2015) helps us to answer sub-RQ 3, which compares the degree to which the digital euro can address the risks and issues related to Bitcoin.

5.5 Mapping of trust factors in digital currencies

We build upon the Cryptocurrency Trust Model by Elsokkary et al. (2022) by integrating institution-based trust factors (Zarifis et al., 2014, 2015; McKnight et al., 2002), and economic and socio-technical trust factors in currencies (Wonneberger & Mieg, 2012). Thus, table 5 provides a comprehensive list encompassing internal and external trust factors that are relevant for digital currencies including CBDCs and cryptocurrencies. This fulfills sub-RQ 1, which posited the question of what mechanisms establish trust in digital currencies. Based on a systematic literature and theoretical review on trust in digital currencies, we establish that the trust characteristics listed in table 5 are mechanisms that play a crucial role in ensuring and increasing trust in digital currencies.

It must be noted that some of these factors pertain to cryptocurrencies (Elsokkary et al., 2022) while others pertain more generally to digital or virtual currencies (Zarifis et al., 2015). To answer the main RQ of this thesis, we seek to put these mechanisms to the test to see which are most relevant to fostering trust in the digital euro, which is a form of a digital currency, namely a CBDC. Thus, the trust factors identified in table 5 will guide the present thesis' Delphi study interview questions.

A few adjustments have been made to the way we have categorized and structured the internal and external trust factors and their respective characteristics. Firstly, economic (hard) and socio-technical (soft) trust factors in currencies by Wonneberger and Mieg (2012) have been categorized under internal trust factors. Elsokkary et al. (2022, p. 77) have argued that liquidity is difficult to classify as it is neither an external nor internal feature but more of a matter of

policy. In our theoretical framework in table 5, we consider Wonneberger and Mieg's (2012) trust factors in currencies which include liquidity as internal factors along with technological trust factors. Since internal trust factors by Elsokkary et al. (2022) are defined as features that developers have direct control and influence over, we argue that in the context of the digital euro, trust factors in currencies by Wonneberger and Mieg (2012) fit under this definition.

'Image' by Wonneberger and Mieg (2012) has been placed under social trust factors on the basis that the emotional attachment that individuals develop towards a currency represents a dispositional trust factor beyond the control of developers, in this case, the ECB. 'Clarity' and 'Support from major players' by Elsokkary et al. (2022) have been placed under institution-based trust factors, specifically, under structural assurance. These factors directly pertain to regulations, laws and institutional mechanisms that influence trust. 'Presence of other systems,' also mentioned by Elsokkary et al. (2022), is closely related to 'support from major players,' and as such, is enclosed in brackets next to it. We have also included a "*studies*" column in table 5 which lists prior studies from our systematic literature review that support these trust factors and their relevance in the context of CBDCs (e.g., digital euro) or cryptocurrencies (e.g., bitcoin).

Table 5: Mapping of trust factors in digital currencies

Table 5: Mapping of Trust factors in digital currencies (CBDCs and Cryptocurrencies)			
	Trust factors	**Characteristics of trust factors**	**Studies**
External trust factors	Social trust factors	Perceived risks Perceived benefits Subject matter expertise (-) Image	Elsokkary et al. (2019); Gupta et al., (2023); Wonneberger and Mieg (2012); Tronnier et al. (2023); Knittel et al., (2019); Gao et al., (2016); Akpaku (2021); Toufaily (2022); Sas & Khairuddin (2015)

	Institution-based trust factors	Situational normality	General structural normality Competence (functionality) Benevolence (helpfulness) Integrity (reliability) Digital currency adoption Digital currency reputation	McKnight et al. (2002); Zarifs et al. (2014, 2015) Toufaily (2022); Sad & Khairuddin (2017); Marella et al. (2019); Albayati et al. (2020); Marella et al. (2020); Arli et al. (2020); Elsokkary et al. (2019)
		Structural assurance	Digital currencies Government backed currency DC payment system Payment intermediary DC P2P infrastructure Self-imposed regulation External Regulation Clarity (-) Support from major players (presence of other systems) (-)	McKnight et al. (2002); Zarifs et al. (2014, 2015); Toufaily (2022); Elsokkary et al. (2019); Auinger and Riedl (2018); Albayati & Rho (2020); Knittel et al. (2019); Shahzad et al., (2018)
Internal trust factors	Technological trust factors (of cryptocurrencies)		**Performance** Effectiveness, Efficiency, Resource Consumption, Time and Space (Timing, Space, Volume, Throughput)	Elsokkary (2022); Tronnier et al., (2023); Ma et al., (2022)
			Portability Installability, Adaptability, Coexistence.	Elsokkary (2022);
			Dependability Maintainability of the Code (Understandability, Changeability, Testability), Robustness, Frequency and Severity of Failure, Stability, Objectivity or Impartiality, Completeness at Point of Creation, Consistency, Durability, Recoverability, Reliability, Availability (Resilience, Redundancy, Scalability)	Elsokkary (2022); Marella et al. (2019); Ali et al., (2022); De Filippi et al. (2020); Ma et al. (2022)
			Identity	Toufaily (2022); Elsokkary (2022);

		Authentication, Authorization, Attributes, Storage, Manageability, Non-repudiation, Scalability	Marella et al. (2019); Ali et al., (2023)
		Security (-) Authentication, Authorization, Integrity, Confidentiality	Elsokkary (2022); Toufaily (2022); Marella et al. (2019); Ali et al., (2023); Ma et al. (2022)
		Privacy (-) Confidentiality, Anonymity, Unobservability, Unlinkability, Pseudonymity, Undetectability	Elsokkary (2022); Toufaily (2022); Ali et al. (2023); Tronnier et al. (2022); Sas & Khairuddin (2017); Ma et al. (2022)
		Decentralization / Centralization	Elsokkary (2022); Saiedi et al., (2021)
	Economic (hard) trust factors of currencies	Liquidity;	Wonneberger and Mieg (2012)
		Fungibility	Wonneberger and Mieg (2012)
		Stability (-)	Wonneberger and Mieg (2012); Knittel et al., (2019)
	Socio-technical (soft) trust factors of currencies	Backing	Wonneberger and Mieg (2012)
		Credibility	
		System security (against economic crises)	
		Manageability (low transaction costs)	

6. Findings

6.1 Delphi study: round 1

The following section details the findings derived from the panel interviews conducted during the first Delphi round. The findings are structured in the following order according to the trust factors in table 5: social trust factors, institution-based trust factors, technological trust factors, economic trust factors, and socio-technical trust factors. The findings are also discussed in relation to findings from previous literature in line with the deductive research method of this thesis.

Social trust factors

Perceived risks of the digital euro

A number of perceived risks were identified among the panelists, which we further coded according to the following descriptive codes: financial risks, lack of user knowledge, privacy risks, and centralization.

Financial risks were identified by two panelists. Panelist 2 expressed that financial stability of the digital euro would be a risk for the greater society since central banks will carry the risk of a bank run as the issuer of the digital euro. The panelist compares this risk to the existing financial system where commercial banks bear similar risks. Another panelist also identified financial risks, specifically related to inflation, as being a perceived risk of the digital euro. The panelist's reason for this was associated with their dispositional belief about the ECB's ability to effectively manage inflation. This corroborates Gupta et al. (2023, p. 10) who found financial risk to have significant influence over trust in the digital rupee (CBDC). This underscores the importance of designing a digital euro that mitigates these financial risks that may prevent users from trusting the digital euro.

"... if we think of the digital euro as a central bank issuing some kind of digital currency, then there is the risk of a bank run" - Panelist 2, fintech lawyer

"Do I trust their ability to do a good job and not really, I do not think they're doing a good job on the inflation part." - Søren Laurits Nielsen, CEO of Bitcoin Suisse Denmark

Lack of user knowledge of the purpose for the digital euro was expressed by two panelists as a potential perceived risk among users that could hinder adoption and likely lead to further risks such as security attacks. However, the panelists did not express whether these perceived risks would likely influence trust in the digital euro.

"... biggest risks are that we as users don't get the right information about what is the purpose of it having a digital euro" - Panelist 1, blockchain consultant

"And if you don't understand why we need a digital euro, then people don't want to adopt it." - Panelist 1, blockchain consultant

"... if we are not really literate, the people who are going to use it, then maybe there will be more hacks of those old people accounts and they'll be fully bankrupt" - Somnath Mazumdar, Assistant Professor at CBS

Privacy was considered a perceived risk that received consensus among all panelists. Privacy risks were underscored as a perceived risk particularly for Europeans where data privacy is considered a significant priority. A panelist also described that users would perceive it as a totalitarian method of control where no privacy is guaranteed from central authorities:

"... biggest risks in having this CBDC (...) but specifically in the euro area we are very concerned about our privacy and our and our data" - Panelist 1, blockchain consultant

"... the first one that comes to mind is definitely the issue of privacy," - Sarah Palurovic, Executive Director at the Digital Euro Association

"... people basically saying this is just another 1984 scenario coming true towards a Society of total transparency." - Sarah Palurovic, Executive Director at the Digital Euro Association

Centralization was also discussed as a significant factor that would potentially increase the perceived risk of the digital euro. The access that central authorities have of users' transaction history and their potential ability to enforce control on the usage of one's digital euro was identified as a significant perceived risk for users' autonomy and freedom. The panelists explained that these risks are what they have observed from social media posts about CBDCs. This confirms the DC reputation factor by Zarifis et al. (2015) which says that the reputation of a digital currency can be influenced by media reports and other external sources, which can influence overall trust. Centralized storage of personal data was also discussed as a perceived risk, and this was mentioned in direct comparison to decentralization, which implies that this is a unique risk to the digital euro compared to cryptocurrencies like bitcoin.

"... from what I see on social media (...) they think that a digital euro is basically just so they can monitor all transactions" - Panelist 1, blockchain Consultant

"...they could if they are the author of the smart contract, and they design it such they could actually just take your money or block them or freeze them." - Søren Laurits Nielsen, CEO of Bitcoin Suisse Denmark

"So if you have data in the digital setting and it's all stored, not decentralized, but centrally somewhere, of course that's going to be a risk" - Sarah Palurovic, Executive Director at the Digital Euro Association

Perceived benefits

Panelists had differing opinions regarding the perceived benefits of the digital euro. Some highlighted its functionality, security, and reduced costs for institutions, while two panelists expressed their uncertainty about its benefits for users.

"Honestly, most people will not see a benefit." - Sarah Palurovic, Executive Director at the Digital Euro Association

"... people will not care whether it's a European solution and that they're using to transact money with most people will not care that it is actually central bank money." - Sarah Palurovic, Executive Director at the Digital Euro Association

"What the end users will get it and it is not very much clear." - Somnath Mazumdar, Assistant Professor at CBS

In terms of functionality, the panelists identified portability, offline payments, and ease of transactions as perceived benefits of the digital euro. Thus, there was consensus among panelists that the primary advantages of the digital euro would stem from its unique functionalities, which are absent in other payment methods.

"... cash is horrendous to have in your wallet" - Panelist 1, blockchain consultant

"... some of the benefits are that you could potentially have offline payments depending on how they build it and the features they implement." - Panelist 1, blockchain Consultant

"It's a lot of money to pay to just move the electronic money from one place to another and this can be done with a digital currency (...) A lot faster and a lot cheaper too." - Panelist 1, blockchain consultant

"... I think easy to use (...) provided they are technically literate, to a good extent." - Somnath Mazumdar, Assistant Professor at CBS

The potential for the digital euro to reduce costs for institutions was also mentioned as a perceived benefit compared to other means of payment today. The panelists underscore that digitalization can promote efficiency that is currently lacking in ways of processing, auditing, and printing paper money.

"it's very difficult for the banks to manage let's say 5 or 7000 Danish kroner in cash because there's so much KYC, AML related to processing cash payments." - Panelist 1, blockchain consultant

"So having something digital, whether the audit trail, is completely transparent, (...) can really make it a lot cheaper" - Panelist 1, blockchain consultant

"... the ECB might have less printing cost because you know, print cost a lot." - Somnath Mazumdar, Assistant Professor at CBS

Lastly, perceived benefits in terms of greater security of the digital euro were mentioned by two panelists.

"(you) don't get mugged because you don't have cash on you." - Panelist 1, blockchain consultant

"... for the end user side it could be kind of a less having a less counterfeit." - Somnath Mazumdar, Assistant Professor at CBS

Subject matter expertise

In terms of whether knowledge of the underlying technology is required to trust the digital euro, consensus was reached that such knowledge is not required for trust. Panelists who held this view emphasized that the lack of technical expertise has seldom deterred individuals from using existing financial systems. Moreover, panelists deemed other factors to be more important for user trust, such as effectively communicating the advantages and incentives associated with using the digital euro. This finding corroborates Khalifa et al.'s (2019) who found that other factors are needed to incentivize trust when technological understanding is lacking among users for a technology like blockchain that they have limited experience using.

"*People don't understand any technology at all, and we don't understand the technology that allows us to have digital money in our bank accounts or how our credit card works or anything."*
- Panelist 2, fintech Lawyer

"for most users, let's say in Denmark, it will just be another version of mobile thing. They don't know how it works in the 1st place" - Søren Laurits Nielsen, CEO of Bitcoin Suisse Denmark

"... I'm not sure if it's communicating what blockchain is that can push this into the right direction, but it's more an understanding of why a digit retail digital euro can benefit the users,"
- Panelist 1, blockchain Consultant

This was also apparent when panelists were asked about the importance of technical expertise for the digital euro to be trusted in comparison to bitcoin. One panelist (Interviewee 2) expressed that the trust issues in bitcoin has more to do with other factors such as its reputation rather than people's lack of technical understanding of the technology. Another panelist, as quoted above, also compared it to that of existing payment systems like "mobilepay" which users do not shy away from using due to a lack of technical understanding. These findings are coherent with Gao et al. (2016, p. 1664)'s who found that non-bitcoin users attributed lack of technical understanding as the reason for not using bitcoin but found it to not be an issue for them to adopt and trust electronic payment methods like credit cards.

"To begin with, I don't think that people don't trust Bitcoin because they don't understand the technology. I think Bitcoin has some reputational risk or it's more of a Bitcoin reputation," - Panelist 2, fintech lawyer

Institution-based trust factors

Situational normality

The degree to which the environment surrounding the digital euro is appropriate and favorable for the user to use and trust the digital euro was only commented on by one panelist. However, the comments provide valuable perspectives on the importance of situational normality. The panelist highlighted the fact that the digital euro's user environment is familiar and integrated or compatible with existing financial systems makes the digital euro easier to trust.

"... it's not some opaque Internet money and some weird website that you have to log into and use a completely new account or bank to then open your account," - Sarah Palurovic, Executive Director at the Digital Euro Association

Competence (functionality), Benevolence (helpfulness) and Integrity (reliability)

These trust factors of situational normality by McKnight et al. (2002; 2011) were not fully addressed or discussed by the participants. The reason for this may be that these characteristics are difficult to address when the digital euro has yet to be launched and the participants have no real experience using the digital euro, making it difficult to refer to concrete examples of features of the digital euro that fulfill these three trust aspects. However, panelists did discuss aspects such as user experience (UX) to be important for enhancing trust, which suggests that functionality and helpfulness of the digital euro as a technology will be important to consider in the design of the digital euro.

"(If) UX is integrated with the existing systems, or the app is especially well made, I can see some benefits there." - Sarah Palurovic, Executive Director at the Digital Euro Association

"... not having to do like identification authentication every single time that you're using your money, that's going to be important just from the user experience side of things." - Sarah Palurovic, Executive Director at the Digital Euro Association

DC reputation

The reputation of digital currencies, specifically cryptocurrencies, was discussed by panelists as a factor that could potentially influence trust in the digital euro. Panelists were largely in consensus that the preexisting biases or distrust that they have of cryptocurrencies, notably bitcoin, could taint their views and their likelihood to trust the digital euro. This confirms Zarifis et al.'s (2014) trust factor on DC reputation and parallels that of Khalifa et al. (2019) who have argued that trust in blockchain technology is influenced by prejudices and experiences. In the case of the digital euro, we can conclude from the responses that reputation of cryptocurrencies, rooted in individual experiences and prejudices, can influence trust in the digital euro. For this reason, panelists underscored the need for the ECB to ensure that the digital euro is marketed and communicated as a currency that is different from cryptocurrencies.

"... cryptocurrencies are providing a negative view on a digital euro because everyone thinks it's a digital currency similar to a cryptocurrency and so again it's a lot about the communication of separating cryptocurrencies to CBDC's." - Panelist 1, blockchain consultant

"*I don't think that the European Commission (...) will market the digital euro as a cryptocurrency, so I don't think it would have the issues of being somehow associated with the things that we don't trust and that is cryptocurrencies." - Panelist 2, fintech Lawyer*

"So they might think that the digital euro is very similar to Bitcoin, and if they already don't understand Bitcoin, I think that will negatively affect the way that they see the digital euro," - Sarah Palurovic, Executive Director at the Digital Euro Association

"Yeah, I guess it's better to trust the digital euro than some random Bahamas exchange, right?" - Søren Laurits Nielsen, CEO of Bitcoin Suisse Denmark

Structural assurance

When asked about structural assurance measures and aspects of the digital euro in comparison to bitcoin, panelists acknowledged that bitcoin has some drawbacks that can hinder user trust. Those drawbacks that were mentioned pertained to the DC payment system and P2P infrastructure, such as the speed of transactions and privacy issues related to bitcoin's blockchain network. This confirms previous literature findings on users' perceived risks of bitcoin. Furthermore, panelists discussed whether these drawbacks affecting trust in bitcoin would be addressed in the design of the digital euro. Panelists shared the viewpoint that the digital euro should offer faster transactions and prioritize user privacy in P2P interactions. This sentiment underscored the collective preference for a digital euro, marking a notable contrast with the perceived shortcomings of bitcoin.

"... the current blockchain is really not suited for processing thousands of transactions per second or per minute," - Søren Laurits Nielsen, CEO of Bitcoin Suisse Denmark

"Bitcoin has a privacy issue related to your peers. All your peers can see whatever you buy or where you buy stuff, but (...) with the digital euro you would have the opposite" - Panelist 2, fintech Lawyer

"...I would rather have somebody in the government knowing what I'm buying or where I'm buying stuff, than having my colleagues know it." - Panelist 2, fintech Lawyer

Regulation

There was strong consensus among panelists that regulation would not be the most important trust factor for the digital euro. Panelist 2 underscored the nature of trust in fiat currencies relies on people's faith and trust in the government and issuers of the currency. This confirms Wonneberger and Mieg (2012)'s theory on the importance of socio-technical trust factors of first currencies like the euro which today is backed by the good faith of the citizenry in terms of the validity of the currency and the issuers behind them. This is further supported by another panelist who alluded to people's pre-existing trust and faith in institutions, namely the European

Union as being an important factor in people's trust in the digital euro. Thus we can observe that in terms of structural assurance, the digital euro being a government backed currency benefitting from people's pre-existing beliefs and faith in their institutions is considered a stronger influential trust factor than regulatory clarity or support.

"No, I don't think regulation will do anything in fostering trust because (...) money itself right now is not really regulated at all," - Panelist 2, fintech lawyer

"... the whole concept about Fiat money is that the only thing you have to trust isn't the currency. You have to trust the government (...) Regulation won't save you." - Panelist 2, fintech lawyer

"... as a citizen wanting to adopt the digital euro (...) I would assume that when it comes from the ECB and from within the European Union, (...) that of course it complies with our very own regulation." - Panelist 1, blockchain consultant

"I do not have a lack of trust in the ECB. (...) I'm sure they are trustworthy, and they're backed by nations." - Søren Laurits Nielsen, CEO of Bitcoin Suisse Denmark

When asked about the importance and clarity of regulation for the digital euro in comparison to bitcoin, panelists believed that regulation is not a significant trust factor for either asset. This is in contrary to previous literature findings which have reported that regulation is a drawback for bitcoin users and non-users in terms of their ability to trust bitcoin. The same finding can be applied to the digital euro as summed up in the aforementioned analysis, suggesting that regulation as an external trust factor will likely not be as important to consider in the influence of trust in the digital euro compared to other external or internal trust factors.

"The reason we don't trust Bitcoin, I don't think it's because of regulation." - Panelist 2, blockchain consultant

Support from major players and Credibility

In discussing the relevance of Elsokkary et al.'s (2022) external trust factor, namely support from major players, we found some overlap in the discussion on the credibility factor belonging

to the socio-technical trust factors by Wonneberger and Mieg (2012). There was clear consensus among panelists that the pre-existing trust in the institutions and actors in the existing financial ecosystem would positively influence trust in the digital euro. Institutions that were mentioned include trust in the government, the ECB, and financial intermediaries like MasterCard. Thus, the presence of institutional actors and their credibility among users are equally, if not more important for fostering trust in the digital euro. This confirms Tronnier et al. (2021, p. 8) who also found a strong correlation between pre-existing trust in the ECB and trust in the digital euro, which the authors explained is because the ECB is more trusted in their responsibility to develop the digital euro compared to unknown entities. Compared to Bitcoin whereby panelists pointed to its reputation as a major source of its drawbacks, the digital euro is able to benefit from its strong credibility and high institutional trust among its European citizens. We can conclude that support from major players is a cryptocurrency trust factor that also translates the digital euro and can address the reputational drawbacks of bitcoin.

"I think it would be associated with my MasterCard in a way and people trust MasterCard, right?" - Panelist 2, fintech lawyer

"The EU has that; we trust our governments more or less like some countries more than others." - Panelist 2, fintech lawyer

***"**... since it's coming from an institution like the ECB, (...) we have had central banks for the past 200 years (...) So I mean, we have a lot of trust no matter what people say." - Panelist 1*

"So generally, our institution works." - Søren Laurits Nielsen, CEO of Bitcoin Suisse Denmark

"... certainly, the fact that commercial banks are going to be the ones distributing the digital euro, I think is going to help because there's already a level of trust that is filled with the customers." - Sarah Palurovic, Executive Director at the Digital Euro Association

Technological trust factors

Performance

The importance of performance in terms of efficiency and effectiveness. Panelists emphasized the importance of ensuring that the ease of use is greater for the digital euro compared to other existing means of payments. Similarly, the necessity of creating an inclusive digital euro where people can effectively have access regardless of demographic location was noted by a panelist as a feature that could increase trust in the digital euro. Offline payments were also considered as a trust-enhancing feature by some panelists. There was a lack of clear consensus on these trust factors, hence they have been included in the survey for the second round of our Delphi study.

"From eastern parts of Europe to all the people in remote villages, do all have access?" - Somnath Mazumdar, Assistant Professor at CBS

"I've identified a finality as one of the most trust building factors. That's of course a big one only with offline payments. (...) I think that would foster trust" - Sarah Palurovic, Executive Director at the Digital Euro Association

"... it should be able to do offline payments because sometimes you're in the middle of a mountain in France (...) but there's no Internet connection" - Panelist 1, blockchain consultant

Dependability

The importance of ensuring dependability in designing the digital euro was discussed with respect to the impartiality of the code and the underlying technology of the digital euro. The need to ensure that the technology that underpins the digital euro is not designed in a way that favors the agenda of certain actors, in this case, the ECB. The ability for users to be able to depend on their digital euro without the risk of losing their financial sovereignty, control and access to their money was deemed an imperative feature to establish user trust in the digital euro. The dependability factor did not reach majority consensus during the first Delphi round, and hence has been included in the subsequent delphi round.

"... it really comes down to what do they actually program, how they design these smart contracts that underpin the CBDC because they could put all sorts of controls into it" - Søren Laurits Nielsen, CEO of Bitcoin Suisse Denmark

"they could (...) control who owns what and also block your money (...) if they are the author of the smart contract." - Søren Laurits Nielsen, CEO of Bitcoin Suisse Denmark

Security

Security as a trust factor was discussed by panelists in relation to the security of data storage of the ECB. Panelists considered centralized data storage to be a security risk due to its vulnerability of potential cyber-attacks and failures, and suggested alternative security infrastructure such as cloud computing, multi-layered security system and quantum computing. This theme also alludes to the trust factor on decentralization/centralization, as the respondents suggest that a non-centralized security infrastructure is key for the digital euro to be trusted. This confirms that security is not only an important trust factor for cryptocurrencies like bitcoin but also imperative for CBDCs, namely the digital euro. Our finding builds upon Tronnier et al. (2023, p. 12) who found that security must be a prerequisite for intended usage of the digital euro. However, the degree to which security mechanisms will be important to foster trust in the digital euro did not reach a clear consensus among the panelists, and thus was considered a non-consensus issue.

" ... cloud computing is the main aim to replace the centralized system because centralized systems are much more vulnerable. So if you are making these centralized ECB based, (...) then how secure are they?" - Somnath Mazumdar, Assistant Professor at CBS

"So hopefully there will be ways to make CBDC quantum computing safe and the same possibly for Bitcoin, though I do think that CBDC if actually have an edge over that" - Sarah Palurovic, Executive Director at the Digital Euro Association

Based on these responses, it is evident that the panelists advocate for a security design that does not bear the vulnerabilities associated with centralized systems. Gross et al., (2021) suggest

that privacy-by-design can help to increase user trust as private data would be stored by the end-user rather than in a centralized system. This can help to boost user confidence by eliminating the need for users to trust in a centralized authority to maintain privacy protections, as well as any threats of large-scale data breaches (ibid). This solution will be discussed in the discussion chapter.

Identity

Respondents also recognized the importance of identity authentication and authorization for the digital euro. This was discussed in relation to KYC and AML features, which respondents considered to be important features to establish trust. The reason for their importance was discussed in relation to bitcoin, in which one panelist asserted that the digital euro must ensure that identities of people are verified which bitcoin does not do. However, the importance of allowing access to the digital euro for people who are not able to easily provide KYC details was also underscored. Hence, the exact design or mechanisms needed for identity verification or the degree of importance for the digital euro was not clearly established. Furthermore, AML capabilities were also mentioned as a trust enhancing feature that would mitigate illicit activities; however, whether the digital euro would effectively address bitcoin's

"... everyone can join (bitcoin) and here we want to make sure that it's primarily people living in the EU, but we also want to be able to provide refugees who don't have ID's, don't have anything with some kind of means of payment so they can have 50 or €100 a day they can, they can use without any KYC." - Panelist 2, fintech lawyer

"Can we know that all the people that have laundered a lot of money and are tax evading, that's really important for us, for fostering trust in the system it's not something illegal. - Panelist 2, fintech lawyer

The responses stressing the need for strict user authentication features raise the question of whether an account-based system is the most trustworthy option as they rely on third-party verification of user identity and account balances. From a financial inclusion perspective, token-based CBDCs are more universally accessible as anyone is able to obtain a digital signature

(Auer and Böhme 2020). However, as underscored by Garratt et al. (2020), it is flawed to think of account-based and token-based as mutually exclusive options. For instance, Bitcoin embodies both systems whereby the use of private-keys for verification resembles that of account-based verification practices whilst the verification of past bitcoin to mitigate double-spending is characteristic of the token-based system. A possible solution would be to employ a hybrid model that integrates both token-based and account-based verification protocols concurrently. In fact, the ECB's (2022, p. 10) prototype briefing revealed that the digital euro has been prototyped on a token-based model using UTXO (Unspent Transaction Output), resembling bitcoin in its use of cryptographic keys. However, the private key is stored by the wallet service provider instead of the end-user. This solution is further discussion in our discussion chapter.

Decentralization (blockchain based)

Whether the digital euro should employ a centralized or decentralized architecture was also a topic of contention among the panelists. Some panelists were of the opinion that the digital euro should be blockchain-based to foster trust. In that case, the panelists believed that it would be able to compete with the advantages of bitcoin that make it trustworthy which is its decentralized network that promotes transparency, security, and impartiality due to its independence from central bank monetary policies. One panelist further emphasized this by characterizing bitcoin's userbase as people who are critical of traditional monetary systems and their policies. By adopting a decentralized architecture, the digital euro would be able to gain the trust of bitcoin and cryptocurrency users who place greater trust in technologies like cryptography rather than human agents and institutions.

"...if the digital euro will be a somewhat blockchain or DLT based then the risks compared to Bitcoin would be small." - Panelist 2, fintech lawyer

" ... those people that are very much into crypto, (...) it's going to foster less trust because they've already started to view the entire monetary system (...) with different lens, (...) So it's

made them more skeptical towards central bank policies and money." - Sarah Palurovic, Executive Director at the Digital Euro Association

"We trust in the math and crypto behind it."- Søren Laurits Nielsen, CEO of Bitcoin Suisse Denmark

On the other hand, the advantages of a centralized, non-blockchain based infrastructure in terms of trust was also underscored by panelists. The ability to control economic measures like inflation was noted as an advantage to the centralized architecture that would help to establish trust in the digital euro compared to bitcoin. However, as there was not a full consensus on which architecture is best suited for the digital euro to foster trust, it is taken up again in the second round of the delphi.

"... that is a big risk to take on for so many citizens and for a currency that is currently already struggling with the inflation environment and so on." - Sarah Palurovic, Sarah Palurovic, Executive Director at the Digital Euro Association

Privacy

The importance of privacy features for the design of the digital euro was the only trust factor that reached full consensus among the panelists. This confirms that Elsokkary et al.'s (2022) theory on privacy as an internal trust factor in cryptocurrency to also play a crucial role in fostering trust in the digital euro, also confirming existing CBDC studies (Tronnier et al., 2021; Ma et al., 2022; Tronnier et al., 2023; Tronnier et al., 2022). However, we note that the panelists acknowledged that the level of importance or priority to instill privacy and anonymity features in the digital euro was equal universally across the European union. Panelists underscored countries like Germany to prioritize anonymity in payments while other countries like Scandinavia to be less concerned about anonymity as they have greater trust in their local institutions. Thus, we note that although there is a consensus on the importance of privacy for the digital euro, this is also context dependent based on the demographic that is concerned in the European union.

"... privacy for some countries and anonymity in payments would be very important for a country like Germany and less important for us in Scandinavia." - Panelist 2, fintech lawyer

"... digital euro just as my MasterCard right now is a lot more private for me, like in the way I want privacy to be, then Bitcoin is." - Panelist 2, fintech lawyer

"... we (europeans) are very keen to keep our data safe and don't share it with anyone" - Panelist 1, blockchain consultant

This observation on privacy has important implications for the digital euro. To design a digital euro that caters to a large demographic of people with different views on privacy would mean that the ECB needs to be flexible in how privacy is integrated into the digital euro. Gross et al. (2021) proposes a two-tiered CBDC system consisting of transparent and private CBDC accounts whereby the central bank deposits CBDCs into users' transparent accounts and users can deposit those CBDCs into their private accounts. The authors propose that the private CBDC accounts will allow for users to conduct fully private, semi-private, and fully transparent transfers, which will comply by AML by, for example, implementing transfer limits without revealing sensitive transfer details (ibid). Accommodating for different tiers of privacy options is also endorsed by the Digital Euro Association (2023), which suggested a two-tier based system to address this question on privacy, whereby low-value payments would have a higher degree of privacy whereas higher value payments would have a lower degree of privacy. These design options will be discussed in the discussion chapter.

Economic trust factors

Fungibility

When asked about the importance of fungibility, few panelists acknowledged its relevance in the context of the digital euro. The limited emphasis on fungibility as a trust factor contrasts with the findings of Wonneberger and Mieg (2012), who identified fungibility as a crucial trust factor for the Euro in comparison to gold. However, one panelist discussed whether the digital euro should be account-based or token-based to be considered more trustworthy.

Hereunder, it was posited that the digital euro should be account-based, rather than token-based as the latter would add unnecessary complexity, especially given the that the digital euro may already be hard to understand in itself. Despite the deviation from Wonnegerber and Mieg's (2012) definition of fungibility, the subject of whether trust will be fostered by an account-based digital euro will be examined for further consensus in the second round of our Delphi study. Panelist 1 mentioned the importance of ensuring the fungibility between the digital euro and the euro, underscoring the importance of ECB to ensure that users have confidence in seamless exchange and convertibility between these two currencies.

"Fungibility is obviously a big one (...) I think the Digital Euro being account based would foster trust more than a token based (digital currency)" - Sarah Palurovic, Sarah Palurovic, Executive Director at the Digital Euro Association

"... we're going to introduce a digital euro. That's already one big step and then saying it's going to be token-based. Most people wouldn't necessarily wrap their head around both of these step" - Sarah Palurovic, Sarah Palurovic, Executive Director at the Digital Euro Association

"... in terms of stability, of course it needs to make sure that it's always pegged one to one (...) it needs to be trusted that no matter what, I can always trade my one digital euro to €1.00 coin" - Panelist 1, blockchain consultant

Liquidity

We found the opinions on whether liquidity will foster trust in the digital euro to be slightly more ambiguous. One panelist expressed concern regarding the potential liquidity challenges faced by banks, although it remains uncertain from this statement why the panelist considers it an issue for banks and whether it will have any effect on the overall trustworthiness of the currency. However, we can observe similarities with the financial perceived risks discussed earlier in our findings whereby panelists expressed issues such as bank runs to be a possible risk.

"... liquidity, of course that's going to be a big issue for banks." - Sarah Palurovic, Sarah Palurovic, Executive Director at the Digital Euro Association

On the contrary, other panelists indicated doubt on the likelihood of the digital euro facing any liquidity challenges at all. The reasoning was mainly based on the premise that the digital euro is issued by the central bank, which until now has not proven to have any issues with ensuring liquidity for the currencies that they issue. Lastly, one panelist expressed that liquidity won't be constituting an important design factor, as it is a feature that the users will care about.

"There's no difference between the digital euro and Fiat currencies, right? (...) So (...) if you're looking at the problem from the ECB to the bank in that aspect, I think it is quite easy to handle liquidity" - Somnath Mazumdar, Assistant professor at CBS

"But I'm thinking because in what circumstance would digital euro not be liquid? (...) because they're issued by the Central bank, I don't think that would be issue ever," - Panelist 2, fintech lawyer

"It's a specialist topic (...) I think they don't care" - Søren Laurits Nielsen, CEO of Bitcoin Suisse Denmark

None of the panelists' statements aligned directly with findings by Wonneberger and Mieg (2012) who deemed liquidity as a crucial trust factor for the traditional Euro. Rather, panelists deemed liquidity to be a given as it is issued by the ECB. This finding corroborates Tronnier et al. (2022, p. 9) whereby hard trust factors, including stability and liquidity, were found to be less influential on willingness to use the digital euro than soft trust factors. The authors reason this as being that panelists take for granted as banknotes issued by the ECB have proven to be highly stable and liquid, which reduces any real concerns for the digital euro (ibid). In this way, soft trust factors were seen as more important for individuals in assessing the digital euro (ibid). Due to the rather unclear statement from the panelists, we do not yet consider liquidity to have reached consensus. Therefore, we will be including it for further analysis in the second round of the Delphi study. Here we aim to better test its relevance, by explicitly asking whether it will be considered an important trust factor from a user standpoint.

Stability

There was a clear consensus amongst the panelists that stability would constitute an important factor in establishing trust in the digital euro. This is coherent with the findings from Shahzad et al. (2018), which suggest that a lack of backing can negatively impact trust in cryptocurrencies. It is further aligned with the findings from Wonnegerber and Miel (2012), which highlights stability as an important element for a trustworthy currency. As all members of the panel stated the importance of stability for trust in the digital euro, the factor has reached consensus in the first round of the Delphi study. Stability will therefore not undergo any further analysis during the second Delphi round.

"We want currency or money to be kind of stable" - Panelist 2

"... in terms of stability, of course it needs to make sure that it's always pegged one to one (...) it needs to be trusted that no matter what, I can always trade my one digital euro to €1.00 coin" - Panelist 1, blockchain consultant

"Then there is the rampant speculation part. People generally do not like." - Søren Laurits Nielsen, CEO of Bitcoin Suisse Denmark

"... it's going to be a stable currency as much as any Fiat currency can be really" - Sarah Palurovic, Executive Director at the Digital Euro Association

"... too little adoption is also not good (...) too much adoption could definitely hurt the stability of the currency." - Sarah Palurovic, Executive Director at the Digital Euro Association

To ensure stability, one panelist underscored the imperative of controlling adoption levels. The importance of controlling the level of adoption is also explained by the panelists' comparison to the euro as they argue that the digital euro should maintain the same degree of stability as the euro. The reason for the Euro's stability can be attributed to its large user base across the eurozone. Thus, this consensus leads us to argue that the ECB may benefit from adoption of the digital euro that is steady enough to encourage and maintain a large userbase. Ways in which the ECB can incentivize the adoption of the digital euro are further discussed in the discussion chapter.

However, these findings must be considered in light of the perceived risks discussed under external trust factors whereby a few panelists underscored potential financial risks including inflation. What we can synthesize from these contrasting findings is that the panelists seem to agree that stability of the digital euro will be imperative for trust, but it does not undermine the fact that the digital euro, just like the euro, relies solely on the citizenry's full faith in the ECB to do a decent job at maintaining stability of the euro (wonneberger and Mieg, 2012). In other words, Europeans cannot be fully assured or promised that the euro will be affected by economic downturns or shocks in the near future.

Socio-technical trust factors

Manageability

Two panelists expressed that the cost associated with using the Digital Euro will play a significant role in its perceived trustworthiness. This is coherent with Wonneberger and Mieg (2012), who posits manageability is an essential trust factor and additionally found manageability to be a hard trust factor for the Euro. The panelists emphasized the importance of ensuring that the digital euro is not more expensive to utilize than existing means of payments, and that there should be no additional costs incurred on users when converting between currencies. Since only two panelists confirmed the manageability of the digital euro to be important for trust, it has not yet reached consensus. The cost associated with the digital euro will therefore be further analyzed in the second round of the Delphi study to determine the possibility of reaching consensus.

"The fact that the digital euro is going to be free for citizens to use, I think that is a big one" - Sarah Palurovic, Executive Director at the Digital Euro Association

"*... the most important thing would be the cost of transfer and the cost of possession, right? So how cheap would it be to do payments and how cheap would it be to have to hold those assets?" - Panelist 2, fintech lawyer*

"Is there an exchange rate that you have to pay when you exchange your euro or your digital euro (...) such features will definitely be important" - Panelist 2, fintech lawyer

Others

Upon analyzing the responses from our panelists, we abductively retrieved a total of five trust-related themes that were not covered by our theoretical framework (table 5), namely cultural differences, communication, User Experience (UX) and User Interface (UI), environmental sustainability, and financial inclusivity. These abductive findings will be analyzed in the subsequent section.

Cultural differences

The first theme derived from the interviews pertains to the impact cultural differences may have in determining the most trustworthy design of a digital euro. Two panelists mentioned the necessity of considering cultural differences amongst Europeans, when trying to reach consensus on the most desired trust factors in designing the digital euro. This was also found by Tronnier et al. (2023, p. 13), in which their respondents underscored the importance of cultural upbringing on attitudes towards payment solutions.

"I think there will be a lot of features that would be important for different areas in Europe (...) we're totally opposite of each other in what we believe is important for design of such things" (...) - Panelist 2, fintech lawyer

"Anonymity in payments would be of course very, very important for a country like Germany and less important for us in Scandinavia" - Panelist 2, fintech lawyer

"They should do local and regional surveys (...) to get an understanding of what is important for the Danish people? What is important for the for the German people? (...) and so on." - Panelist 1, blockchain consultant

Despite "cultural differences" not having reached consensus, we have decided to omit it from further analysis in the second round of the Delphi study. This decision is rooted in the fact

that this factor belongs to the external trust factor according to the definition by Elsokkary et al. (2022). It would be considered an external trust factor because it is not something that developers have direct control over, but it pertains to users' backgrounds and experiences which could also potentially influence their perceived benefits and risks of the digital euro.

Communication

The second theme derived pertains to how communication about the digital euro likely will be a key factor in establishing trustworthiness amongst users. Three panelists stressed that establishing trust in the digital euro will be highly contingent upon effectively communicating its purpose and features to the European population:

"So I think that in order to gain trust from European citizens. I think they should start out with communicating" - Panelist 2, fintech lawyer

"it's more of a communication issue rather than the technical solution and feasibility because the solutions are there, (...) they're working, but people don't trust it." - Panelist 1, blockchain consultant

"I think the key to this lies in the communication strategy" - Sarah Palurovic, Executive Director at the Digital Euro Association

In addition to emphasizing the importance of a communication strategy, the panelists further elaborated on what the communication optimally should convey to the public. All three expressed that establishing a clear distinction and disassociating the digital euro with any form of cryptocurrency, would play a critical role in fostering trust:

"If you market it as something blockchain crypto asset based, it will probably have some risk concern related to like association with something that we don't trust somehow (...) I would say if people associated the digital euro with crypto assets like Bitcoin, that would probably be an issue" - Panelist 2, fintech lawyer

“And so again it's a lot about the communication of separating cryptocurrencies to CBDC's” - Panelist 1, blockchain consultant

"Draw the Devil's face on Bitcoin and make sure they're distancing themselves from anything that's happening in the crypto world” - Sarah palurovic, Executive Director at the Digital Euro Association

One interviewee further indicated how transparent communication will be crucial in terms of fostering trust, and that it is important for the European Central Bank (ECB) to provide comprehensive and transparent information about both the benefits and drawbacks of the digital euro:

“(...) if you are willing to introduce a new form of agency, it has to be well discussed, transparently saying good things, bad things, properly stated measures and then only you can go ahead” - Somnath Mazumdar, Assistant professor at CBS

Altogether, 4 participants suggested communication to be an important factor in establishing trust in the digital euro. Thus, a consensus has been reached during the initial round of the Delphi study. Yet, the relevance of communication in relation to our research objective is subject to discussion, let alone how to categorize it in our theoretical framework (table 5). Firstly, communication cannot be considered an internal trust factor as it is not something that the developers of the digital euro have direct influence over. The ECB can only be responsible for part of the overall communication disseminated about the digital euro, as journalists, media outlets, and individuals retain the freedom to say anything they see fit. This indicates that communication is at least partially an external trust factor, which as previously mentioned will be excluded for further analysis in our thesis. Thus, communication will be omitted going forward. Nevertheless, this discovery is interesting and stands to have a significant impact and influence on trust in the digital euro and will therefore be touched in the discussion chapter as a way to complement our discussion on how the ECB should design the digital euro to foster trust.

UX and UI

The third theme addresses the UX and UI of the digital euro. Two panelists underscored the importance of ensuring that the digital euro functions as a convenient and seamless payment method, where users are not required to undertake any extra measures compared to other means of payment on the market. This builds upon Tronnier et al. (2023, p. 11)'s findings that perceived ease of use and high usability constituted important perceived benefits and antecedents to using the digital euro over established payment methods.

"... it needs to be extremely easy for me to just open an app and then pay (...) I should not experience any issues compared to using cash" - Panelist 1, blockchain consultant

"So I'm not making it more cumbersome than regular payment methods that we know today are" - Sarah Palurovic, Executive Director at the Digital Euro Association

Several specific features were proposed that could potentially aid in enhancing the user experience of the digital euro. It was suggested to incorporate the digital euro into preexisting payment infrastructure to simplify its usage, and also eliminate the need for users to undertake cumbersome steps to use the digital euro. This was further emphasized by a proposal to facilitate the usage of the digital euro via a waterfall approach, wherein users don't realize they are using a digital euro, but it simply just happens through the payment system.

"(...) if the UX is integrated with the existing systems or the app is especially well made, I can see some benefits there. I also think that the seamlessness is really going to help (...) so the waterfall and the reverse waterfall mechanism is going to help in not really making people realize what type of money they're currently using" - Sarah Palurovic, Executive Director at the Digital Euro Association

"I don't need to log in and I don't need to sign into eight different places and so on" - Panelist 1, blockchain consultant

As only two of the panelists stressed UX and UI as important features for establishing trust in the digital euro, it will be further analyzed in the second round of the Delphi study, to see if it can reach consensus amongst the broader panel of experts.

Enviromental sustainability

The fourth theme inductively derived pertains to the environmental sustainability of the digital euro. Specific examples of how the digital euro could be designed to be environmentally sustainable were not given; however, it was underscored as a factor that could positively influence users' perceptions of the digital euro. Sustainability would fall under internal trust factors according to Elsokkary et al. (2022), since developers can promote sustainability through the digital euro's technical design. It was not clear whether a sustainable design would be correlated with trustworthiness, and thus this factor is included in the second Delphi round to assess whether panelists' general opinion on its importance for establishing trust in the digital euro.

"Sustainability. I mean, just from like marketing perspective that would be nice to have" - Sarah Palurovic, Executive Director at the Digital Euro Association

Financial inclusivity

The final theme derived concerns the inclusivity of the digital euro and was highlighted by two of the panelists. They underlined that a trustworthy digital euro should be available to all people within Europe, irrespective of their socio-economic group, geographical location and technical expertise. This could be argued to overlap with UX and functionality trust factors previously discussed, since the way that these two factors are designed could promote financial inclusion. Yet, inclusion was only mentioned by two of the panelists, meaning it did not reach consensus in the first round of the Delphi study. It will therefore be included in the second round.

"... designing an actually inclusive digital euro is important" - Sarah Palurovic, Executive Director at the Digital Euro Association

"I think it has to be inclusive and we need to think more about the vulnerable portion of society (...) not all people in Europe have iPads or smartphones," - Somnath Mazumdar, Assistant professor at CBS

"Out of big cities, you can see the technical bandwidth is also kind of reducing right?" - Somnath Mazumdar, Assistant professor at CBS

Summary of findings from Delphi round 1

The findings from the first round of the Delphi study can be summarized according to internal and external trust factors. Within internal trust factors, privacy and stability reached consensus among the panelists, constituting consensus-issues. Conversely, 13 internal trust factors, including features identified abductively (UX/UI, financial inclusion, environmental sustainability), did not reach consensus and thus are considered non-consensus issues. These non-consensus issues will be brought forward to the second Delphi round to further assess their degree of importance for the design of the digital euro. As for external trust factors, we found strong consensus that regulation would not yield a significant influence on trust. Notably, the pre-existing credibility of the ECB and support from institutional actors in the digital euro ecosystem were identified as pivotal trust factors that are able to address the drawbacks of bitcoin in terms of its reputation. While opinions varied on other components of our external trust factors, they will not be further explored in the second Delphi round. Cultural differences and communication which we found abductively are also omitted from the second Delphi round. The reason for this decision is that the RQ concerns how the digital euro should be designed, which can more effectively be answered by achieving greater consensus among the non-consensus issues identified among the internal trust factors, as these are design features that the developers of the digital euro have direct influence over. The discussion chapter will, however, delve into these external trust factors to complement our recommendations for the ECB in shaping the design of the digital euro.

6.2 Delphi study: round 2

The following section details the findings derived from the survey conducted during the second round of the Delphi study. We present the findings from the survey in which panelists were asked to rank 13 internal trust factors in order of their importance for fostering trust in the digital euro (see survey in appendix 4, p. 51). Through a consensus analysis, we categorize the findings

into features that achieved consensus as 'very important' or 'less important' (see table 6). Furthermore, we categorize and discuss the findings on the characteristics that did not reach consensus among the panelists, which we have labelled ‘no consensus’ (see table 6).

Findings from this second Delphi round are also discussed in relation to previous literature and our theoretical framework (table 5) in line with the deductive aspect of our abductive research method. We are also considering the findings from the first round of the Delphi study, as well as the rationale for their individual rankings provided by the panelists in the survey (see appendix 5, p. 53-57)

Consensus analysis

To better understand the level of consensus across the panelists in how they ranked the 13 trust factors, we performed a statistical analysis by calculating Kendall's W coefficient of concordance. This analysis is particularly useful as it provides a value indicating the level of consensus among numerous submitted responses (Bar-Ilan, J. 2005). The Kendall’s W coefficient came out to be a value of 0.29, which falls well below the predetermined threshold of 0.7 suggested by Okoli and Pawlowski (2004) as an indication of a significant degree of consensus (see chapter 4.7, p. 43). The lack of overall consensus of the rating scale warrants an examination of the consensus levels for each trust factor. This allows for a more informed analysis of the perceived importance of each of the 13 trust factors.

The trust factors are therefore each classified according to three categories: 'most important for trust’, 'least important for trust’ and ‘no consensus’ (see table 6). The categories are based on both the mean ranking score and variance of each trust factor (see appendix 6.2). For example, the trust factor, "security" had a mean ranking score of 3.8 and a variance of 5.7. According to our metric, this factor is considered "most important for trust".

The threshold for the variance was chosen to be 15, based on the 3. quartile of the dataset. This is a sound metric to utilize in our scenario as the obtained dataset is limited in size and thus does not allow a high degree of discrimination as would often be the case if the dataset was

larger. 75% is therefore considered to be a fitting threshold for the variance. The true value of the 3. Quartile is 14.7, but since the factor "Liquidity equivalent to the traditional euro" has this exact value for its variance, we have tweaked the variance threshold to 15, and thus included the factor in a consensus group. An additional reason as to why we placed this variable within the consensus threshold is its low mean value, which we also want to have an impact on our analysis.

Together, the mean values and variance provide greater insights into the overall ranking and the degree of consensus or divergence for each trust factor, helping us to better understand the importance of each trust factor for establishing trust in the digital euro in order to answer the main RQ.

Table 6: Ranking of trust factors based on level of importance

Category	**Trust factors**
Very important for trust: *Factors ranked among the top 66% of the 13 factors in the survey (>8.71) and has a degree of consensus in their respective rankings (variance less than 15)*	• Security mechanisms (Cloud computing, multi-layered security system) • Seamless UX and UI • Authentication of user identity • Traceability of transactions to mitigate illicit activities & money laundering • Liquidity equivalent to the traditional euro • Financial inclusion • Zero transaction fees • Account based
Less important for trust: *Factors ranked among the bottom 33% of the 13 factors in the survey (<8.71) and has a degree of consensus in their respective rankings (variance less than 15).*	• Offline payments • Environmentally sustainable
No consensus:	• Decentralized architecture

Factors without consensus in their respective rankings (variance greater than 15).	• Centralized architecture • Impartiality of the code

1. More important for trust

Based on the consensus analysis described above, a total of 8 out of the 13 surveyed trust factors were considered under the category of "very important for trust". Out of these 8 trust factors, 6 of them adhered to the pre-determined trust factors in our theoretical framework (table 5), specifically security, identity, dependability, as theorized by Elsokkary et al. (2022), and fungibility, liquidity and manageability as theorized by Wonneberger and Mieg (2012). This finding suggests that these trust factors are just as important for building trust in centralized currencies like the CBDC as much as they are for cryptocurrencies and regular currencies. The remaining 2 trust factors (UX/UI and financial inclusion) were derived abductively and are found to be important trust-building mechanisms for the digital euro.

A crucial observation made from this category is that most of the 8 trust factors lean towards soft trust factors (technological and socio-technical trust factors) rather than hard trust factors (economic). Notably, soft trust factors garnered more attention and meaningful discussion during the Delphi study, while certain hard trust factors like liquidity were seemingly taken for granted and unquestioned by the panelists. Despite the semi-structured interview format allowing room for panelists to introduce additional features they considered important for building trust in the digital euro, our findings from the high priority list predominantly consist of soft trust factors.

This observation aligns with Tronnier et al.'s (2022, p. 9) assertion that in Euro area regions where institutional trust is high, such as the Scandinavian region represented by our panelists, hard trust factors are viewed as less significant compared to soft trust factors. Therefore, the emphasis in designing the digital euro should be on ensuring that the soft trust factors identified in the high priority list are meticulously addressed. We also see the emphasis

on soft trust factors in the qualitative comments provided by the panelists in the second round of the Delphi study explaining their rationale behind their ranking choices. The extracts of their comments below show that emphasis is given to trust factors like security, UX, and transaction fees (manageability) and less so on hard (economic) trust factors.

"Thus, strong security practices must be used to gain wider adoption. Strong security features help minimize online threats including distributed denial-of-service (DDoS) attacks and should lower vulnerability. It must also secure personal and financial information" - Somnath Mazumdar – Assistant professor at CBS

"Security aspects and zero glitches in transaction settlement are all the average citizens will care about. All outward facing components such as the UX are what will transfer the trust from the bank note to the CBDC. Zero remuneration is another factor: the digital euro benefits from being a new form of what already exists and what people are familiar with." - Sarah Palurovic, Director at the Digital Euro Association

"I believe it is given that it should be account-based for example. Also, to ensure trust from a user perspective, the traceability of transactions may not support that although it should…" - Panelist 1, blockchain consultant

2. Less important for trust

The consensus analysis revealed that 2 out of the 13 trust factors have been considered in the category of "less important for trust". These trust factors are offline payments and environmental sustainability. The former adheres to the trust factor on performance, as theorized by Elsokkary et al. (2022) while the latter was identified abductively in the first Delphi round. It is important to note that these two trust factors are only considered less important in comparison to the rest of the trust factors that the panelists were asked to rank in order of importance. Thus, these trust factors should not be disregarded or undermined but instead be given less priority in designing a trustworthy digital euro compared to the 8 trust factors which were identified as very important.

Offline payments

Offline payments were categorized under "less important for trust," due to its mean score of 10.2. This trust factor falls under the performance trust factor which Elsokkary et al. (2022) identified as an internal trust factor for cryptocurrencies. It also adheres to the functionality factor by McKnight et al. (2011), as offline payment is a type of functionality that the digital euro would be able supply to ensure task completion (i.e., the settlement of payments in the absence of internet connectivity). We can thus conclude that performance and functionality also have a degree of relevance for ensuring trust in the digital euro as they do for cryptocurrencies and regular fiat currencies.

However, despite its functional relevance, panelists perceived it to be less critical to trust in the digital euro. The reason could be that offline payments and other performance-related functionality features primarily enhance the convenience of the digital euro, rather than substantially contributing to increased trust. Thus, we posit based on this finding that prioritizing trust-enhancing factors like privacy over convenience-oriented factors such as offline payments are essential to ensure a trustworthy digital euro.

Environmentally sustainable

Environmental sustainability was also categorized as "less important for trust," garnering a mean score of 10. Although this factor was only mentioned by one panelist during the first Delphi round, the consensus analysis revealed a notable consensus among the panelists that this would constitute a rather important trust factor for the digital euro. A potential reason for the lower importance assigned to this factor can be explained by the panelist's (Sarah) reasoning from the first Delphi round in which the panelist stated that ensuring an environmentally sustainable digital euro could be a positive feature to consider but more in terms of marketing purposes. Based on this reasoning and the panelists' ranking score, we argue that environmental sustainability is a desirable feature but not perceived to be an imperative factor in terms of establishing trust. Hence, this feature should not be given high priority when designing the digital euro to maximize trust.

3. No consensus

Three out of the 13 trust factors failed to achieve consensus. All three items were initially derived deductively from our theoretical framework. As the rankings of each of these trust factors differed significantly across the panelists, we refrain from categorizing them as either "more important" or "less important" for trust in the digital euro. A conclusive determination in this regard would require an additional iteration of the Delphi study. To understand the reasons behind this lack of consensus, we analyze the panelists' qualitative comments explaining their choice of for ranking.

Decentralized / centralized architecture

The panelists assigned the following ranks to the decentralized architecture: 1, 1, 11, 12, and 13. Giving it a mean value of 7.6, and the largest variance among all factors, totaling 36.8. Centralized architecture received rankings of 12, 5, 1, 13, and 13, which generated a mean value of 8.8 and the second highest variance, totaling 30.2. Evidently, a clear lack of consensus prevails amongst the panelists regarding which design architecture is more important for establishing trust in the digital Euro.

This finding is not surprising, given that the ranking options entailed both decentralized and centralized architectures as options, which consequently resulted in panelists ranking them on opposite ends of the spectrum of importance since it is not possible for the digital euro to encompass both as its fundamental architecture. Additionally, the rankings reflect the influence of panelists' professional backgrounds. Those with institutionally oriented roles tended to favor centralized rankings, whereas panelists with a cryptocurrency background leaned toward prioritizing decentralization. The following two extracts demonstrate this pattern that we observed. Søren, the CEO of Bitcoin Suisse Denmark, ranked decentralization first on the ranking scale, and underscores in their reasoning that no unique benefit is provided if it is not decentralized or blockchain-based. In contrast, Panelist 2, a fintech industry lawyer highlighted the trust-securing potential of a centralized currency, particularly among Nordic populations who already have high levels of trust in their institutions.

"If it is not decentralized/blockchain it is just a bank account at ECB. What would I need that for? I would love to replace some of the traditional crypto stablecoins with these" - Søren, *CEO of Bitcoin Suisse Denmark*

"The Nordic countries are renowned for their significant level of trust in their respective public institutions. Consequently, I have identified a centralized system led by a public authority as the foremost factor in fostering trust in a digital euro infrastructure." - Panelist 2, fintech lawyer

Impartiality of the code and design

The panelists assigned the following ranks to impartiality of the code and design: 2, 9, 3 and 12 Giving it a mean value of 5.6, and a variance totaling 21.3. We again found that panelists with institutionally oriented roles ranked this factor lower than panelists with a cryptocurrency background. This trust factor is a sub-feature of Elsokkary et al.'s (2022) internal trust factor on dependability, which is a highly relevant trust factor especially for bitcoin considering that a large fraction of bitcoin's user base are individuals who distrust centralized, institutional actors in the financial system (Knittel et al., 2019, p. 14-5; Saiedi et al., 2021, p. 383). However, this factor may not be of high relevance or importance in the context of the digital euro, since achieving complete impartiality is unattainable given that the digital euro is crafted by an institution with specific objectives.

7. Discussion

This section first provides a summary of the main findings from the Delphi study. Thereafter, we present answers to the main RQ of the thesis by providing recommendations for the ECB on how the digital euro should be designed to foster greater trust compared to bitcoin. Recommendations are given based on trust factors that were identified as very important for trust based on the consensus analysis of the second Delphi round, as well as the two internal trust factors that reached consensus in the first Delphi round. The risks associated with bitcoin which

were discussed by the panelists will also be discussed in terms of how they can be mitigated by our design recommendations. The subsequent sections are dedicated to reflections of our theoretical framework and chosen methodology, whereby we will present considerations of its strengths and weaknesses. Lastly, we will address the limitations of our study, while providing suggestions for future research.

7.1 Summary of Delphi study findings

The Delphi study, carried out through two iterative rounds, led us to identify 10 internal trust factors that achieved consensus among the panelists as crucial considerations for the design of the digital euro. Eight of these trust factors are reported in Table 6 under "very important for trust", while the remaining two trust factors (privacy and stability) had achieved consensus among the panelists in the first Delphi round. As mentioned in our analysis of the findings of Delphi round 2, most trust factors that were considered important for the digital euro were "soft" trust factors (technical and social) while fewer pertained to "hard" economic factors, as per the definitions of Wonneberger and Mieg (2012). This finding has important implications for how the digital euro should be designed, as the expert panel are generally in agreement that soft trust factors yield greater influence over trust than economic trust factors.

Furthermore, findings on external trust factors highlighted the notable influence that external factors can play in potentially influencing trust, such as perceived risks, perceived benefits, reputation, and structural assurance. When compared to the drawbacks of bitcoin, our findings deviated from previous literature findings. The panelists identified the primary drawbacks of bitcoin to be related to its reputation and volatility in value, rather than regulatory issues, illicit activity, and lack of technical and subject matter expertise. Hence, design recommendations for the digital euro shall focus more on the two former drawbacks in strengthening the position of the digital euro against cryptocurrencies like bitcoin.

7.2 Recommendations

In formulating our recommendations, we bring forth an important theoretical contribution by Albayati and Rho (2020, p. 9) from our theoretical framework, who describe trust and risks to be inversely related. Following this theory, the recommendations we provide for the ECB are designed to reduce the perceived risks of the digital euro that were identified in the first Delphi round, as well as the risks associated with bitcoin.

1. **Ensuring financial stability**

Stability in value was considered a crucial factor by the panelists for ensuring trust in the digital euro (see Chapter 6.2, table 6). Recommendations to ensure stability must consider the perceived financial risks of the digital euro that were mentioned by the panelists, notably the risk of inflation (see chapter 6.1, p. 66). Although specific recommendations were not provided by the panelists on how to mitigate inflation and maintain a stable currency, it would be beneficial for the ECB to design it in a way that minimizes the damage that inflation and economic uncertainty could potentially have on users who rely on the digital euro. Ensuring the short-term and long-term stability of the digital euro will effectively address the risk of bitcoin's short-term instability, thereby enhancing trust and positioning the digital euro favorably. Likewise, the institutional support that the digital euro benefits from (see chapter 6.1, p. 69) will provide a trustworthy liquidity pool as well as various possible features like fungibility that are not effectively provided by bitcoin.

As mentioned in our analysis, one panelist mentioned the need to maintain a reasonable level of adoption to maintain the stability of the digital euro (see p. 6.1, p. 78-9). Although this is not a design feature, we advise the ECB to consider various incentive mechanisms that can help to foster initial adoption. Examples of such incentives may include the form of free credits when users first install the digital euro onto their wallets, encouraging merchant and retail acceptance of the digital euro through zero transaction fees, allowing for free deposits (i.e., cash to digital euro) at ATMs, and free transactions. However, ways to foster and control the level of adoption require further research to ascertain their effectiveness.

2. **Privacy-enabling transactions**

Privacy was deemed an important trust factor for ensuring trust in the digital euro by all panelists particularly for European citizens that have a lower degree of institutional trust (see chapter 6.1, p. 75). To accommodate differences in privacy preferences among the European citizenry, we recommend a design that allow for users to make low value transactions anonymously. Some examples that were discussed in our analysis include a two-tiered privacy model that can balance security (i.e., AML) and privacy. Such privacy design propositions resonate with the views of the panelists that emphasized the importance of considering the priorities of privacy-concerned euro citizens as well as ensuring security protocols to mitigate illicit activities (see chapter 6.1, p. 63). However, similar to blockchain technology, the primary challenge the ECB will encounter in ensuring security for the digital euro is navigating the blockchain trilemma, which involves balancing security, scalability, and decentralization. The ECB will need to carefully consider which factor may need to be compromised, as there is often a trade-off between prioritizing two of these elements.

With regards to privacy issues of bitcoin, some panelists expressed hesitancy of the transparent nature of bitcoin's public ledger whereby one's bitcoin transaction history is publicly stored and visible to anyone. By designing a non-DLT based digital euro, this drawback can be mitigated so that one's transaction history is only accessible to the end-user, the bank and central institutions. However, further research is needed to determine a privacy model that caters to varying privacy preferences of the European population.

3. **Data security**

Strong security of the digital euro was agreed upon by the panelists as an important trust factor the digital euro (see chapter 6.2, table 6). Specifically, the emphasis was on ensuring the security of data storage systems. The panelists mentioned examples of non-centralized data storage such as cloud computing and multi-layered security systems (see chapter 6.1, p. 71-2). In addition to these examples, our analysis referred to the privacy-by-design approach whereby private data would be stored by the end-user rather than in a centralized system. However,

further investigation is needed to ascertain a security model that best balances the centralization and decentralization, since our panelists did not reach consensus on these two factors (see chapter 6.2, table 6).

4. **Seamless UX and UI**

To ensure a seamless UX and UI, we recommend the ECB to conduct usability testing to identify possible user interface challenges that could hinder users' trust and adoption of the digital euro. The panelists expressed that integrating the digital euro into our existing financial ecosystem would likely increase users' confidence in the digital euro (see chapter 6.1, p. 83-4). Thus, although technical expertise was agreed by the panelists as not a significant issue hindering trust (see chapter 6.1, p. 64-5), the UX and UI should be user-friendly, efficient and easy to navigate. This will also ensure that the UX fosters universal accessibility, catering to all demographics and age groups, which also fulfills the financial inclusion factor that was considered important among the panelists (see chapter 6.2, table 6).

5. **Hybrid account-based and token-based verification system**

The ability to effectively verify user identity and trace transactions to mitigate financial crime was found to be an important trust factor for the digital euro (see chapter 6.1, p. 63). These features are instrumental in addressing concerns about the reputational risks associated with illicit activities that surround Bitcoin and other cryptocurrencies. Based on the panelists' responses, we recommend the ECB to adopt a verification system that does not threaten financial inclusion. For instance, individuals that cannot easily provide proof of identity such as refugees should not face challenges in accessing the digital euro. In light of the importance of financial inclusion as underscored by our panelists (see chapter 6.2, table 6), our analysis discussed the option of adopting a hybrid model that utilizes the verification systems of account-based and token-based systems (see chapter 6.1, p. 72-3). While this may promote a healthy balance between user experience, financial inclusion and robust security and user verification, conducting additional usability testing is advised to determine the type of verification model that

is desirable across different eurozone demographics. As discussed previously, varying priorities for trustworthiness across the eurozone may yield valuable insights through constructive feedback.

7.3 Reflections

The following section will provide a reflective assessment of how well our theoretical framework and choice of methodology aided us in answering our RQs. We will reflect on both strengths and weaknesses while covering what could have been done differently.

Theoretical framework

The findings of this study have implications for the theoretical framework that guided the research. Our theoretical framework (table 5) serves as the foundation for answering our RQ and the analysis of our data. Through an abductive research approach (see chapter 4.3, p. 29), our primary data collection aimed to test the theoretical framework (deductively), while allowing for the potential discovery of novel trust factors (abductively). This section will discuss the strengths and weaknesses identified through the application of our theoretical framework.

Strengths

Due to the limited availability of academic research on trust in the digital euro and CBDCs, we faced the challenge of not being able to rely on concrete theories that were relevant for studying trust in the digital euro. Therefore, we drew upon theories that have been tested in the context of other forms of currencies, such as fiat money and cryptocurrencies. This, however, turned out to be a clear strength for our study, as we managed to deductively validate many of the identified factors in our theoretical framework despite the lack of prior proven relevance. The validation hereof gave a clear justification for how our deductive approach and theoretical framework helped us in addressing our research question.

Weaknesses

While we were able to validate many of the trust factors from the theoretical framework and deemed the deductive part of our research approach effective, it's important to also consider limitations and weaknesses. As the digital euro is such a novel concept it might have been a limitation to mainly utilize a deductive approach to answer our research question. Despite leaving room to explore novel factors through the primary data collection (abductively), this was not the primary focus. We could possibly have identified a broader range of factors not pertaining to the theoretical framework, if we had aimed for a more inductive and exploratory research approach. Yet, we still managed to retrieve five novel factors in the first round of the Delphi study, indicating that the abductive approach was successful, at least to some extent.

Delphi method

Given the significance of our primary data for this thesis, it is crucial to consider the strengths and weaknesses associated with its collection. We utilized an abductive 2-round Delphi study encompassing firstly an interview round and secondly a survey round. Together, the aim was to arrive at a consensus amongst a panel of experts, on what design factors the Digital Euro should include to foster more trust than bitcoin. This section will cover the strengths and weaknesses associated with the employed Delphi method.

Strength

The present study suggests a strong alignment between the adductive Delphi methodology employed and our research philosophies, namely critical realism and pragmatism (see chapter 4.1, page 27-8). Our objective was to thoroughly understand all the trust factors that could correspond to the digital euro, while ultimately also providing practical design recommendations to the ECB. Initially, our focus was on reaching consensus among the panelists, however we discovered that a clear strength of the Delphi study lays in the nuances, and rich insights it can provide on a complex topic such as trust in the digital euro, regardless of having reached consensus. With this method we were able to effectively test trust factors from previous literature, while also assessing new ones. Overall, the Delphi method showed itself to be a valuable method in aiding us to answer our research questions.

Weaknesses

Although the Delphi technique has proven to be beneficial in addressing our primary research question, there are a few limitations to consider. Firstly, how generalizable the findings are, especially as our panel consisted of just five experts. Yet, we did try to mitigate this limitation by carefully selecting a panel of experts with a diverse range of backgrounds. Secondly, the scope of factors we could assess was naturally limited because of the 45-minute interviews. This again underpins how primarily deductive / slightly abductive research approached might have excluded the attention on novel factors, that were not identified in the theoretical framework. Nevertheless, to avoid this being a strong limitation we allowed for the extension of an interview if the panelists had anything additional to add once the questioning was finalized.

7.4 Limitations

The selected panel

The scope of our thesis was to investigate the factors that will influence trust in the digital euro, a digital currency that is intended to be utilized by end-users throughout the vast majority of Europe. However, during the initial round of the Delphi study it was brought to our attention that the cultural and historical differences between European countries might result in varying views of the concept of trust (chapter 6.1 p. 80). Thus, it became apparent that we might lack cultural diversity among the selected panelists, which could pose a potential limitation to our study. The chosen panelists reside primarily in northern Europe, thus it is crucial to acknowledge that the composition of our panel may not adequately reflect what the European population would consider trustworthy. According to Millar et al. (2007), a weakness of the Delphi study is the possibility of bias in the chosen panel. Yet, the intention was to gather a diverse group of specialists, which we managed to do both industry and background wise. Nevertheless, the perspective of more properly representing the European population, needs to be explored further.

7.5 Future research

Future research may derive value from the findings outlined in this thesis, particularly when considering the weaknesses and limitations discussed in the preceding section. To begin with, it is necessary to conduct further research on the three factors that did not reach consensus in the second round. This is deemed important, as the decision regarding their inclusion or exclusion will have a substantial impact on the final design of the digital euro. Secondly, to address the limitation of having a panel consisting primarily of experts from northern Europe, it would be interesting in future research to include a broader representation of Europe. This could potentially aid in ensuring the digital euro doesn't fail in certain countries, while succeeding in others. Lastly, in the theoretical framework we discovered both internal and external factors that could influence trust in digital currencies. However, in the second round of the Delphi survey, we opted to exclusively include the internal trust factors, and exclude all the external ones. This decision was made, as the ECB, whom we are providing guidance to, only possesses direct influence over the internal aspects. Yet, it is considered critical for future research to further investigate the external factors, as they also proved to be vital for establishing trust in the digital euro.

8. Conclusion

The primary goal of this thesis was to determine how the digital euro should be designed by the ECB to foster trust by identifying the most important trust factors for its design. To address this research objective, a primary RQ was established and two corresponding sub-research questions that guided our investigation of the main RQ.

RQ: *How should the digital euro be designed to foster trust compared to bitcoin?*

Sub-RQ 1: *"How and what mechanisms establish trust in digital currencies?"*

Sub-RQ 2: *"To what extent do the trust characteristics of the digital euro address the risks associated with Bitcoin that undermine trust?"*

The primary objective of sub-RQ1 was to identify the trust characteristics that are shared among digital currencies, including both cryptocurrencies and CBDCs. Through a systematic literature review, a theoretical framework was developed comprising a comprehensive list of pertinent trust factors for digital currencies. This framework served as the basis for evaluating and identifying the trust factors most relevant to fostering trust in the digital euro. Thus, the answer to sub-RQ 1 is addressed through table 5 of our theoretical framework, which consists of two overarching themes and five sub-themes: 1) internal trust factors, encompassing technological trust factors, economic (hard) trust factors and socio-technical (soft) trust factors, and 2) external trust factors, including social trust factors and institution-based trust factors.

Sub-RQ2 was established with the purpose of better understanding the limitations associated with trust in Bitcoin, to ensure these would be addressed in the proposed design of the digital euro. A total of seven limitations undermining trust in Bitcoin were identified in our systematic literature review: subject matter expertise, regulatory clarity, institutional support (presence of other systems), security, privacy, and stability in value. These drawbacks of bitcoin were subsequently discussed with the panelists during the first Delphi round, as to how the digital euro can mitigate these limitations. Contrary to previous studies, our findings revealed a consensus that the risks associated with bitcoin primarily revolved around its reputation and volatility in value. The digital euro fulfils these drawbacks of Bitcoin by relying on the pre-existing trust that Europeans have in institutional actors including the ECB, and by our recommendation to back the digital euro one-to-one with the euro, as well as a portfolio of commodities such as gold, oil and/or bitcoin.

To answer our primary research question, a Delphi study of two rounds was conducted to reach consensus among the panelists on the trust factors that the ECB should consider for designing a trustworthy digital euro. Based on a total of ten trust factors agreed upon by the panelists, we devised recommendations for the ECB on the digital euro should be designed for trust whilst also addressing the drawbacks of bitcoin that have been discussed in the present thesis. Our recommendations are as follows:

1. Implement measures to ensure the stability of the digital euro;

2. Privacy-by-design;

3. Privacy-enabled low value transactions;

4. Seamless UX/UI based on field testing among the European population;

5. A hybrid account-based and token-based verification system.

References

Albayati, H., Kim, S. K., & Rho, J. J. (2020). Accepting financial transactions using blockchain technology and cryptocurrency: A customer perspective approach. *Technology in Society, 62*, 101320.

Ali, V., Norman, A. A., & Azzuhri, S. R. B. (2023). Characteristics of Blockchain and its Relationship with Trust. *IEEE Access, 11*, 15364-15374.

Almarashdeh, I. (2018). An overview of technology evolution: Investigating the factors influencing non-bitcoins users to adopt bitcoins as online payment transaction method. *Journal of Theoretical and Applied Information Technology, 96*(13), 3984-3993.

Amaral, G., Prince Sales, T., & Guizzardi, G. (2022, May). Ontological foundations for trust dynamics: The case of central bank digital currency ecosystems. In *International Conference on Research Challenges in Information Science,* 354-371. Cham: Springer International Publishing. 97

Amaral, G., Sales, T. P., Guizzardi, G., & Porello, D. (2019). Towards a reference ontology of trust. In *On the Move to Meaningful Internet Systems: OTM 2019 Conferences: Confederated International Conferences: CoopIS, ODBASE, C&TC 2019, Rhodes, Greece, October 21–25, 2019, Proceedings* (pp. 3-21). Springer International Publishing.

Amos, T., & Pearse, N. (2008). Pragmatic research design: An illustration of the use of the Delphi technique. *Electronic Journal of Business Research Methods, 6*(2), pp133-140.

Akpaku, E. (2021). The Antecedents to the Actual Use of Digital Currencies in Ghana. *International Journal of ICT Research in Africa and the Middle East, 10*(2), 92–110.

Arrow, K. J. (1972). Gifts and exchanges. *Philosophy & Public Affairs*, 343-362.

Auer, R., and R. Böhme. (2020). *The Technology of Retail Central Bank Digital Currency*. BIS Quarterly Review. BIS. https://www.bis.org/publ/qtrpdf/r_qt2003j.pdf.

Auinger, A., & Riedl, R. (2018). Blockchain and trust: Refuting some widely-held misconceptions. T*hirty Ninth International Conference on Information Systems, San Francisco.*

Avizienis, A., Laprie, J. C., Randell, B., & Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. *IEEE transactions on dependable and secure computing*, *1*(1), 11-33.

Baharuddin, R., Singh, D., & Razali, R. (2013). Usability dimensions for mobile applications-a review. *Res. J. Appl. Sci. Eng. Technol*, *5*(6), 2225-2231.

Bank of International Settlements (BIS). (2021a). *Central bank digital currencies: user needs and adoption*. BIS (Report No. 3). https://www.bis.org/publ/othp42_user_needs.pdf.

Bank of International Settlements (BIS). (2021b, June 23). *Central bank digital currencies herald a new chapter for the monetary system.* BIS. https://www.bis.org/press/p210623.htm

Bank of International Settlements (BIS). (2020, October 09). *Central bank digital currencies: foundational principles and core features.* BIS. https://www.bis.org/publ/othp33_summary.pdf

Bank of International Settlements (BIS). (2021c, June 23). *III. CBDCs: an opportunity for the monetary system.* BIS. https://www.bis.org/publ/arpdf/ar2021e3.pdf

Bar-Ilan, J. (2005). Comparing rankings of search results on the web. *Information Processing & Management*, *41*(6), 1511–1519.

Bijlsma, M., van der Cruijsen, C., Jonker, N., & Reijerink, J. (2021). What triggers consumer adoption of CBDC?. *De Nederlandsche Bank Working Paper No. 709.*

Bouoiyour, J., & Selmi, R. (2019). Beyond the Big Challenges facing Facebook's Libra. Working paper or preprint. https://hal.archives-ouvertes.fr/hal-02309316

Brady, S. R. (2015). Utilizing and Adapting the Delphi Method for Use in Qualitative Research. *International Journal of Qualitative Methods, 14*(5).

Bramer, W. M., Rethlefsen, M. L., Kleijnen, J., & Franco, O. H. (2017). Optimal database combinations for literature searches in systematic reviews: a prospective exploratory study. Systematic reviews, 6, 1-12.

Budree, A., & Nyathi, T. N. (2023). Can Cryptocurrency Be a Payment Method in a Developing Economy?: The Case of Bitcoin in South Africa. *Journal of Electronic Commerce in Organizations, 21*(1), 1–21.

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics, 36*, 55–81.

Central Bank of Ireland. (n.d). "*A Digital Euro."* https://www.centralbank.ie/financial-system/payments-and-securities-settlements/a-digital-euro.

Chuenjitwongsa, S., Poolthong, S., Bullock, A., & Oliver, R. G. (2017). Developing common competencies for Southeast Asian general dental practitioners. *Journal of Dental Education*, *81*(9), 1114-1123.

Chung, L., & do Prado Leite, J. C. S. (2009). On non-functional requirements in software engineering. *Conceptual modeling: Foundations and applications: Essays in honor of john mylopoulos*, 363-379.

Craggs, B., & Rashid, A. (2019, May). Trust beyond computation alone: Human aspects of trust in blockchain technologies. In *2019 IEEE/ACM 41st International Conference on Software Engineering: Software Engineering in Society (ICSE-SEIS),* 21-30.

D. H. McKnight, V. Choudhury, and C. Kacmar. (2002). 'Developing and validating trust measures for E-commerce: An integrative typology. *Inf. Syst. Res, 13*(3), 334–359.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, 319–340.

De Filippi, P., Mannan, M., & Reijers, W. (2020). Blockchain as a confidence machine: The problem of trust & challenges of governance. *Technology in Society, 62*, 101284.

Digital Euro Association. (2023, August 4). *CBDCs & Privacy: Considerations for an International Landscape.* YouTube. https://www.youtube.com/watch?v=XY71relWM6A&t=4s

Dyer, J. H., & Chu, W. (2003). The Role of Trustworthiness in Reducing Transaction Costs and Improving Performance: Empirical Evidence from the United States, Japan, and Korea. *Organization Science*, *14*(1), 57–68.

Elsokkary, N., ur Rehman, M. H., Suhail, S., Kaindl, H., & Svetinovic, D. (2022, August). Trust Evaluation of Blockchain-Based Cryptocurrencies: The Cases of Bitcoin and Diem. In *2022 International Balkan Conference on Communications and Networking (BalkanCom),* 73-77.

European Central Bank (ECB). (n.d.-a). *"Why do we need a digital euro?" ECB.* https://www.ecb.europa.eu/paym/digital_euro/why-we-need-it/html/index.en.html

European Central Bank (ECB). (n.d.-b). *"What would a digital euro be?" ECB.* https://www.ecb.europa.eu/paym/digital_euro/features/html/index.en.html

European Central Bank (ECB). (2022, September). "Progress on the investigation phase of a digital euro." ECB. https://www.ecb.europa.eu/paym/digital_euro/investigation/governance/shared/files/ecb.degov220929.en.pdf.

European Central Bank (ECB). 2023. "Progress on the Investigation Phase of a Digital Euro – Third Report." https://www.ecb.europa.eu/paym/digital_euro/investigation/governance/shared/files/ecb.degov230424_progress.en.pdf

European Central Bank (ECB). (2020, October) *Report on a digital euro.* ECB. https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf

Ferraris, D., & Fernandez-Gago, C. (2020). TrUStAPIS: a trust requirements elicitation method for IoT. *International Journal of Information Security*, *19*(1), 111-127.

Fisch, C., & Block, J. (2018). Six tips for your (systematic) literature review in business and management research. Management Review Quarterly, 68, 103-106.

Fishbein, M., & Ajzen, I. (1977). Belief, attitude, intention, and behavior: An introduction to theory and research. *Addison-Wesley, Reading, MA*.

Fletcher, A.J. and Marchildon, G.P. (2014) 'Using the Delphi method for qualitative, participatory action research in Health Leadership', *International Journal of Qualitative Methods*, *13*(1), 1–18.

Gao, X., Clark, G. D., & Lindqvist, J. (2016). Of Two Minds, Multiple Addresses, and One Ledger: Characterizing Opinions, Knowledge, and Perceptions of Bitcoin Across Users and Non-Users. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (CHI '16), 1656–1668.

Gambetta, D. (1988). Can we trust Trust? In: Gambetta, D. (Ed.), Trust: Making and breaking cooperative relations. Blackwell, New York, 213–237.

Garratt, R., M. Lee, B. Malone, and A. Martin. (2020). *Token- or Account-Based? A Digital Currency Can Be Both.* Federal Reserve Bank of New York. Liberty Street Economics. https://libertystreeteconomics.newyorkfed.org/2020/08/token-or-account-based-a-digitalcurrency-can-be-both/.

Georgieva, K. (2022, February 9). *The Future of Money: Gearing up for Central Bank Digital Currency.* International Monetary Fund. https://www.imf.org/en/News/Articles/2022/02/09/sp020922-the-future-of-money-gearing-up-for-central-bank-digital-currency.

Gordon, T. A. (2006). Pease RT Delphi: An efficient, "round-less" almost real time Delphi method *Technological Forecasting and Social Change*, 73 (4) , 321-333.

Gross, J., Sedlmeir, J., Babel, M., Bechtel, A., & Schellinger, B. (2021). Designing a central bank digital currency with support for cash-like privacy. http://dx.doi.org/10.2139/ssrn.3891121

Griffith University. (2021). *How can I use Google Scholar to enhance my systematic-style review?* https://staffhelp.secure.griffith.edu.au/app/answers/detail/a_id/4415/~/how-can-i-use-google-scholar-to-enhance-my-systematic-style-review%3F

Hasson, F. (2000). Research guidelines for the Delphi Survey Technique. *Journal of Advanced Nursing, 32*(4), 1008.

Hoff, K. A., & Bashir, M. (2015). Trust in automation: Integrating empirical evidence on factors that influence trust. *Human factors*, *57*(3), 407-434.

International Monetary Fund (IMF). (2023, February 16). *Nigeria: 2022 Article IV Consultation-Press Release; Staff Report; and Statement by the Executive Director for Nigeria* (Country Report No. 2023/093). https://www.imf.org/en/Publications/CR/Issues/2023/02/16/Nigeria-2022-Article-IV-Consultation-Press-Release-Staff-Report-and-Statement-by-the-529842

Ivankova, et al (2009). Mixed methods. Qualitative research in applied linguistics: A practical introduction, 23, 135-161.

Jacobs, M. (2021). How implicit assumptions on the nature of trust shape the understanding of the blockchain technology. *Philosophy & Technology, 34*(3), 573-587.

Jalan, A., Matkovskyy, R., Urquhart, A., & Yarovaya, L. (2023). The role of interpersonal trust in cryptocurrency adoption. *Journal of International Financial Markets, Institutions and Money*, *83*, 101715.

Jalava, J. (2003). From norms to trust: The Luhmannian connections between trust and system. *European journal of social theory*, *6*(2), 173-190.

Karam, A., (2023, August 17). "*Central Bank Digital Currency (CBDC) and blockchain enable the future of payments."* IBM. https://www.ibm.com/blog/central-bank-digital-currency-cbdc-and-blockchain-enable-the-future-of-payments/

Kim, C., Tao, W., Shin, N., & Kim, K. S. (2010). An empirical study of customers' perceptions of security and trust in e-payment systems. *Electronic commerce research and applications, 9*(1), 84-95.

Knittel, M., Pitts, S., & Wash, R. (2019). The Most Trustworthy Coin. *Proceedings of the ACM on Human-Computer Interaction, 3*(CSCW), 1–23.

Korfiatis, Y. (2020). "D-Euro: Issuing the Digital Trust." *Social Science Research Network*.

Khalifa, D., Madjid, N. A., & Svetinovic, D. (2019, June). Trust requirements in blockchain systems: a preliminary study. In *2019 Sixth International Conference on Software Defined Systems (SDS),* 310-313.

Landeta, J. (2006). Current validity of the Delphi Method in Social Sciences. *Technological Forecasting and Social Change, 73*(5), 467–482.

Lankton, N. K., McKnight, D. H., & Thatcher, J. B. (2014). Incorporating trust-in-technology into expectation disconfirmation theory. *The Journal of Strategic Information Systems, 23*(2), 128–145.

Lankton, N. K., McKnight, D. H., & Tripp, J. (2015). Technology, humanness, and trust: Rethinking trust in technology. *Journal of the Association for Information Systems, 16*(10), 1.

Leppanen, A. (2010). *Technology trust antecedents: building the platform for technology enabled performance.* Department of Business Technology Helsinki School of Economics. http://epub.lib.aalto.fi/en/ethesis/pdf/12310/hse_ethesis_12310.pdf

Luhmann, N. (1979), Trust and Power, Wiley & Sons, New York.

Luhmann, N. (1986), Vertrauen. Ein Mechanismus Der Reduktion Sozialer Komplexit€at, Stuttgart: Ferdinand Enke Verlag., Enke, Stuttgart.

Lustig, C., & Nardi, B. (2015, January). Algorithmic authority: The case of Bitcoin. In *2015 48th Hawaii International Conference on System Sciences* (pp. 743-752). IEEE.

Ma, C., Jin, Z., Mei, Z., Zhou, F., She, X., Huang, J., & Liu, D. (2022). Internet of Things background: An empirical study on the payment intention of central bank digital currency design. *Mobile Information Systems.*

Marella, V., Upreti, B., Merikivi, J., & Tuunainen, V. K. (2020). Understanding the creation of trust in cryptocurrencies: The case of Bitcoin. *Electronic Markets*, *30*(2), 259-271.

Matemba, E. D., & Li, G. (2018). Consumers' willingness to adopt and use WeChat wallet: An empirical study in South Africa. *Technology in Society*, *53*, 55-68.

McGimpsey, P., & Broverman, A. (2023, June 28). *Different Types Of Cryptocurrencies Explained.* Forbes Advisor. https://www.forbes.com/advisor/au/investing/cryptocurrency/different-types-of-cryptocurrencies-explained/

McKnight, D. H., & CHERVANY, N. L. (2001). What trust means in e-commerce customer relationships: An interdisciplinary conceptual typology. *Int. J. Electron. Commerce 6*, 2, 35–59.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information systems research*, *13*(3), 334-359.

Melnikovas, A. (2018). Towards an explicit research methodology: adapting research onion model for futures studies. *Journal of Futures Studies*, 23(2), p. 29–44.

Mcknight, D. H., Carter, M., Thather, J. B, & Clay, P. (2011). Trust in a specific technology: An investigation of its components and measures. *ACM Transactions on Management Information Systems, 2*(12), 12–32.

Millar, K., Thorstensen, E., Tomkins, S., Mepham, B., & Kaiser, M. (2007). Developing the ethical delphi. *Journal of Agricultural and Environmental Ethics, 20*(1), 53–63.

Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System." https://bitcoin.org/bitcoin.pdf

Okoli, C. and Pawlowski, S.D. (2004) 'The delphi method as a research tool: An example, design considerations and applications', *Information & Management*, *42*(1), 15–29.

Paré, G., Cameron, A.-F., Poba-Nzaou, P., & Templier, M. (2013). A systematic assessment of rigor in information systems ranking-type Delphi Studies. *Information & Management*, *50*(5), 207–217.

Pavlou, P. A. (2003). Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model. *International Journal of Electronic Commerce, 7*(3), 101–134.

Rogers, E. M. (1962). Diffusion of innovations. New York: Free Press.
Saiedi, E., Broström, A., & Ruiz, F. (2021). Global drivers of cryptocurrency infrastructure adoption. *Small Business Economics*, *57*, 353-406.
Sandhu, K., Dayanandan, A., & Kuntluru, S. (2023). India's CBDC for digital public infrastructure. *Economics Letters*, 231, 111302.
Sas, C., & Khairuddin, I. E. (2015, December). Exploring trust in Bitcoin technology: a framework for HCI research. In Proceedings of the Annual Meeting of the Australian Special Interest Group for Computer Human Interaction, 338-342.
Saunders, M., Lewis, P., & Thornhill, A. (2019). Research methods for business students. Pearson education.
Shahzad, F., Xiu, G., Wang, J., & Shahbaz, M. (2018). An empirical investigation on the adoption of cryptocurrencies among the people of mainland China. *Technology in Society, 55*, 33–40.
Shcherbak, S. (2014). How should Bitcoin be regulated? *European Journal of Legal Studies*. *7*(1) 46-91.
Singh, M., & Mattackal, L. (2023, May 3). Cryptoverse: Digital coins lure inflation-weary Argentines and Turks. *Reuters.* https://www.reuters.com/technology/cryptoverse-digital-coins-lure-inflation-weary-argentines-turks-2023-05-02/.
Smolyansky, E. (2020). *Announcing Connected Papers — a visual tool for researchers to find and explore academic paper*. Medium. https://medium.com/connectedpapers/announcing-connected-papers-a-visual-tool-for-researchers-to-find-and-explore-academic-papers-89146a54c7d4
Soderberg, G., Kliff, J, Bechara, M., Forte, S., Kao, K., Lannquit, A., Sun, Tao., Tourpe, H., and Yoshinaga, A. (2023, September). How Should Central Banks Explore Central Bank Digital Currency? A Dynamic Decision-Making Framework. *FinTech Notes,* (008).
Söilen, K. S., & Benhayoun, L. (2021). Household acceptance of central bank digital currency: the role of institutional trust. *International Journal of Bank Marketing, 40*(1), 172-196.
Stanley, A. (2022). *The Ascent of CBDCs.* International Monetary Fund. https://www.imf.org/en/Publications/fandd/issues/2022/09/Picture-this-The-ascent-of-CBDCs
Stiefmüller, M. C. (2023). *The Digital Euro: A Matter of Trust*. Finance Watch. https://www.finance-watch.org/wp-content/uploads/2023/10/The-Digital-Euro_Policy-Brief_Oct-2023.pdf
Story, V., Hurdley, L., Smith, G., & Saker, J. (2000). Methodological and practical implications of the Delphi technique in marketing decision-making: a re-assessment. *The Marketing Review*, *1*(4), 487-504.

Sveriges Riksbank. (2023, February 1). *On the possibility of a cash-like CBDC.* Riksbank. https://www.riksbank.se/globalassets/media/rapporter/staff-memo/engelska/2021/on-the-possibility-of-a-cash-like-cbdc.pdf

Thompson, J. (2022). A Guide to Abductive Thematic Analysis. *The Qualitative Report, 27*(5), 1410-1421. https://doi.org/10.46743/2160-3715/2022.5340

Thoring, K., Klöckner, H. W., & Mueller, R. M. (2022). Designing the future with the "Delphi design sprint": Introducing A novel method for design science research. *Proceedings of the Annual Hawaii International Conference on System Sciences.*

Toufaily, E. (2022). An integrative model of trust toward crypto-tokens applications: A customer perspective approach. *Digital Business, 2*(2), 100041.

Tronnier, F., & Kakkar, S. (2021). Would You Pay with a Digital Euro? Investigating Usage Intention in Central Bank Digital Currency. *Investigating Usage Intention in Central Bank Digital Currency.*

Tronnier, F., Harborth, D., & Biker, P. (2023). Applying the extended attitude formation theory to central bank digital currencies. *Electronic Markets, 33*(1), 13–13.

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.

Tsiakis, T., & Sthephanides, G. (2005). The concept of security and trust in electronic payments. *Computers & Security, 24*(1), 10–15.

Tyszka, T., & Przybyszewski, K. (2006). Cognitive and emotional factors affecting currency perception. *Journal of economic psychology*, *27*(4), 518-530.

U.S House Committee on Financial Services. (2019). *An examination of facebook and its impact on the financial services and housing sectors.* https://financialservices.house.gov/uploadedfiles/hhrg-116-ba00-20191023-sd002.pdf

Vance, A., Elie-Dit-Cosaque, C., & Straub, D. W. (2008). Examining trust in information technology artifacts: the effects of system quality and culture. *Journal of management information systems*, *24*(4), 73-100.

Varndell, W., Fry, M., & Elliott, D. (2021). Applying real-time Delphi Methods: Development of a pain management survey in emergency nursing. *BMC Nursing*, *20*(1).

Viljanen, L. (2005, August). Towards an ontology of trust. In *International conference on trust, privacy and security in digital business,* 175-184.

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly, 26*(2), xiii–xxiii.

Wonneberger, E. T., & Mieg, H. A. (2012). Trust in money: Hard, soft and idealistic factors in Euro, gold and German community currencies. *Journal of Sustainable Finance & Investment*, *1*(3-4), 230-240.

Wohlin, C. (2014). Guidelines for snowballing in systematic literature studies and a replication in software engineering. In *Proceedings of the 18th international conference on evaluation and assessment in software engineering*, 1-10.

Woudenberg, F. (1991). An evaluation of Delphi. *Technological forecasting and social change*, *40*(2), 131-150.

Zarifis, A., Cheng, X., Efthymiou L. and Dimitriou, S. (2014). Consumer Trust in Digital Currency Enabled Transactions. *Business Information Systems*, *183*, 241-254.

Zarifis, A., Cheng, X., Dimitriou, S., & Efthymiou, L. (2015). Trust in Digital Currency Enabled Transactions Model. *MCIS 2015 Proceedings*. 3.

Zhang, X., & Zhang, Q. (2005). Online trust forming mechanism: approaches and an integrated model. *ACM International Conference Proceeding Series; Vol. 113: Proceedings of the 7th International Conference on Electronic Commerce,* 201–209.