Technology Innovation in Financial Markets: Implications for Money, Payments and Settlement Finality

Ruth Wandhöfer

PhD Thesis in Finance

CASS Business School, City University London and

TIAS Business School, Tilburg University

Department of Finance

July 2019

TABLE OF CONTENTS

Chapter 3:

Chapter 4:

Sarah Connor: "My whole life I've prepared my son to lead in a fight against machines. They last thing I could imagine is that he'd become one of them."

John Connor: "I'm not a man, not a machine... I'm more!"

Terminator Genisys

ACKNOWLEDGEMENTS

On a continuous journey of curiosity I embarked on this PhD as one of my 'must-dos' in life. The topic I chose happens to be in an area that is one of the most dynamic ones, not only influencing the world of finance but also due to permeate all of our lives as we move into the digital age.

It all began while watching Terminator Genisys on a flight to SIBOS in Singapore – a big transaction banking industry conference and gathering - in 2015. As the idea for my dissertation began to ferment in my brain, I started connecting the dots of Terminator Genisys, Minority Report, Matrix and Oblivion – reflecting the potential journey of humankind's future in movie terms. What could technology do to society?

The first evening in Singapore serendipity herself stepped in - Thank You! - as I met, once again, Prof. Ron Berndsen. We were both about to attend an industry evening event when I began a conversation about Bitcoin and distributed computer systems and laid out my plans for the PhD in my usual enthusiastic way. He was immediately captured by the idea and agreed to be my supervisor. Only after some research did I find out that Tilburg University, where Prof. Berndsen was resident professor, collaborated with CASS Business School in London on a joint

Executive PhD degree. This was the opportunity of a lifetime! And so I applied.

Once we began the course I had the pleasure to meet my second supervisor Prof. Barbara Casu. We connected straight away and our conversation often ended up in a mix of English and Italian.

I would like to thank Barbara and Ron for their strong interest, support, passion and friendship. This PhD came at a time of my life when everything was about to change. I am so grateful to Barbara and Ron for their true and continued friendship, for sharing my passion and for helping me to turn my vision into this thesis.

I thoroughly enjoyed my study times in Tilburg and London and our cohort became a really close group of friends. Here I would like to thank the CASS and Tilburg faculty teams and staff, which were of great help and support throughout my research.

Furthermore, this PhD would not have happened without the support of my former employer, Citi.

And of course I would like to extend my gratefulness for the many experts that have contributed to my research, in particular in the area of cross-border payments. Most of them are listed in the Annex to Chapter 3, but special thanks go to Simon, Richard, Klaus, the SWIFT teams, Mark, John and Ken.

Finally, and most importantly, I would like to thank my parents and my family, who believed in me and always understood and nurtured my curiosity to learn, understand and grow.

Ruth

DECLARATION

I herewith grant powers of discretion to the University Librarian to allow the thesis to be copied in whole or in part without further reference to the author.

ABSTRACT

In this thesis we explore the implications of technology innovation across the areas of settlement finality, cross-border payments and money.

As a first step, we investigate the topic of settlement finality in the context of Proof-of-Work (PoW) blockchains, exemplified by Bitcoin. This is of particular importance as final settlement plays a crucial role in removing settlement risk between counterparties in support of financial stability. We extend earlier work in Berndsen (2013) on functional modelling of the theoretical settlement problem. By applying his model we provide a functional interpretation of settlement finality and propose a new encompassing definition of settlement finality, which expands the academic field of payment economics. We also assess whether PoW is functionally superior to the backward looking legal framework for settlement finality.

In a second step we explore whether and how technological innovation, in conjunction with policy measures, can improve the process of correspondent banking cross-border payments. Following the empirical validation of existing shortcomings by using a questionnaire and industry expert focus group sessions, we identify key requirements based on which we develop several design scenarios for the future of cross-border payments. We then evaluate the different models and complement our findings with policy and standards recommendations, outlining a practical way forward for the industry.

Finally we explore an alternative perspective on the future role of central bank money as a retail use digital complement to physical cash. Against a set of future scenarios we develop the rationale for a Eurosystem issued 'Digital Euro' and proceed by delivering a high level blueprint for the design of such a solution. As retail cash payments move into the digital age with the associated challenges for citizens' data, identity as well as financial stability and system security, such a step will become an increasingly relevant consideration for the Eurosystem.

ABBREVIATIONS

ACH = Automated Clearing Houses

AISP = Account Information Service Provider

AML = Anti Money Laundering

APIs = Application Programming Interfaces

ASPSP = Account Servicing Payment Service Provider

BIS = Bank for International Settlements

BTC = Bitcoin

CCP = Central Counter Party

CHIPS = Clearing House Interbank Payments System

CIPS = China International Payment System

CBDC = Central Bank Digital Currencies

CBDFC = Central Bank Digital Fiat Currencies

CLS = Continued Linked Settlement

CPMI = Committee on Payments and Market Infrastructures

CTF = Counter Terrorism Financing

DBM = Digital Base Money

DDoS = Distributed Denial of Service

DL = Distributed Ledger

DLT = Distributed Ledger Technology

DNS = Deferred Net Settlement

DSF = Degree of Settlement Finality

DvP = Delivery versus Payment

EACHA = European Automated Clearing House Association

EBA = European Banking Authority

ECB = European Central Bank

EP = European Parliament

FATF = Financial Action Task Force

FI = Financial Institution

FMI = Financial Market Infrastructure

FSB = Financial Stability Board

FX = Foreign Exchange

GDPR = General Data Protection Regulation

G-SIFIs = Globally Systemically Important Financial Institutions

gpi = Global Payments Innovation

IMF = International Monetary Fund

IoM = Internet of Money

IOSCO = International Organisation of Securities Commissions

IoT = Internet of Things

IPFA = International Payments Framework Association

ISO = International Organization for Standards

KYC = Know Your Customer

KYCC = Know Your Customer's Customer

LEI = Legal Entity Identifier

MAS = Monetary Authority of Singapore

MM = Money Market

NCB = National Central Bank

NSA = National Security Agency

P2P = Peer-to-Peer

PISP = Payment Information Service Provider

PSD2 = Payment Services Directive 2

PMI = Payment Market Infrastructure

PSP = Payment Service Provider

PoW = Proof of Work

PvP = Payment versus Payment

QE = Quantitative Easing

RMA = Relationship Management Application

RTGS = Real Time Gross Settlement

SCA = Secure Customer Authentication

SEPA = Single Euro Payments Area

SFD = Settlement Finality Directive

SIC = Swiss Interbank Clearing

SLAs = Service-Level Agreements

SME = Small and Medium-size Enterprise

SWIFT = Society for Worldwide Interbank Financial Telecommunication

TARGET = Trans-European Real-Time Gross Settlement Express Transfer

TIPS = TARGET Instant Payment Settlement

TPP = Third Party Provider

UETR = Unique End-to-End Transaction Reference

UFM = Uniform Functional Model for the Financial Infrastructure

UTXO = Unspent Transaction Outputs

VC = Virtual Currency

"After this, there is no turning back.

You take the blue pill—the story ends; you wake up in your bed and believe whatever you want to believe.

You take the red pill—you stay in Wonderland, and I show you how deep the rabbit hole goes.

Remember: all I'm offering is the truth."

The Matrix

Chapter 1

Introduction

We live in times of unprecedented change. Since the arrival of the Internet, technology advances have been accelerating rapidly and data has grown exponentially. The speed of technology change combined with increasing efficiencies in computing power (Moore's Law) are the source of new business models and solutions, allowing us to radically reimagine the way our societies will operate in the future. The Internet dominates working and private life alike. As the next step of evolution we are entering the Internet of Things (IoT), where connected machines and systems capture data, learn and ultimately take decisions. Driver-less cars, hyperloops, virtual reality, artificial intelligence, personal robots, cloud computing, quantum computing, self-replenishing fridges and talking holograms are no longer fantasies in movies. 'Back to the Future' is playing out right here, right now in front of our eyes.

With data being the 'oil of the digital era', the financial services industry, like many other industries, is being significantly disrupted as we move into the next big sensation - the Internet of Money (IoM) - essentially a term that alludes to the future of Internet based money and payments. In parallel, innovations in payment systems and services, complemented by regulatory measures to increase competition and consumer protection, have become an important trend around the globe.

Before we develop the three angles of innovation in relation to settlement finality, money and payments, we will first of all introduce the context of technology innovation in the financial system. As a next step, we outline the gaps in extant research that this thesis is planning to address and provide an outline of the dissertation, including the underlying theoretical and empirical studies.

1.1 FROM INTERNET TO CRYPTOCURRENCIES & DISTRIBUTED LEDGERS

Over the last decade, markets have witnessed a systemic crisis and financial meltdown, starting with the bankruptcy of Lehman Brothers in 2008. As a consequence regulators around the world began to set more stringent rules for the financial industry, ranging from capital and liquidity requirements (the Basel 3 framework) to tougher Anti-Money-Laundering (AML) and Counter-Terrorist-Financing (CTF) requirements. Financial Market Infrastructures (FMIs) also became a focal point of regulatory attention, with tighter rules being established around counterparty risk management and settlement finality. Emerging cybersecurity risks became another area of regulatory focus. The result of these measures led banks to become inwardly-focused on compliance triggering the spiralling of costs and opening up the door for technology savvy providers to enter the banking value chain in more efficient ways. Just like other industries in the past – e.g. media, telecommunications etc. – banking came to be disrupted. Crowd-funding, peer-to-peer lending and ultimately platform banking became the 'new kids on the block'. The unbundling of the bank had started in earnest.

In the aftermath of the financial crisis another outstanding innovation appeared on the scene with the arrival of Bitcoin, the first cryptocurrency that operates without the involvement of the financial industry. Bitcoin started as an isolated experiment, endorsed by libertarians that took issue with the way our centralised societies operate. Since 2009 Bitcoin has inspired the creation of thousands of crypto currencies and tokenised assets, which now make up the ever-growing digital financial ecosystem that remains largely outside the control of governments and regulators. Bitcoin's underlying technology came into focus for both the emerging new players as well as the regulated financial industry and was hailed to provide a more secure and efficient way of transferring digital assets or currency.

The Bitcoin blockchain is a specific instance of distributed ledger technology (DLT), which is why in this thesis we will use the more generic term of DLT. Today there are over 100 different types of DLTs, and new developments in this space are continuously growing. The main thing that all of these platforms have in common is the architectural concept of using a shared digital ledger to distribute the process of sharing information across an ecosystem. They do this by providing a single source of data that all of the participants in the network can see, can contribute to, and can trust that it is accurate.

In a complex ecosystem, where there is movement of value or information flowing across the ecosystem - how can the various participants ensure that the records of this movement is captured accurately? Currently the financial system relies heavily on trusted intermediaries or central bodies. The participants all trust that the records kept by the middleman are accurate, and they reconcile their own records with the central records. With some implementations of DLT, such as the Bitcoin blockchain, there is no central authority or intermediary. This is an evolution from a system built on financial intermediaries to one built on financial protocols. DLT provides a different option, where each of the participants in the ecosystem can join a network that automatically captures all of the movement across the network and validates the correct order for that movement to prevent duplication of information or value. The network also has embedded participant verification and uses cryptographic keys to ensure that the holders of these keys have the authority to initiate a transfer. If a particular account does not have the right key, the network will not accept the information being broadcast by that account.

In addition to this disintermediation, DLT has a unique and rich stack of inbuilt capabilities. For example, the distribution of the network's operation makes the overall network more resilient and available as it doesn't have a single point of failure. The ability to customize control of the network is another important capability. The auditable ledger means that once a transaction has been validated and agreed upon to be committed to the ledger, it cannot be removed (Irrevocable) or changed (Immutable). This indelible audit trail makes it valuable for use cases that require verification of existence, process or provenance.

Smart contracts are a further evolution, where DLT can have embedded business logic that can be used to allow for self-executing enforcement of contractual terms that are specified in digital form.

And thirdly, tokenisation allows the creation of a digital wrapper around value (whether that is currency, commodity, or a financial instrument), which can then be transferred across the network in an efficient and secure manner.

This technology phenomenon is leading us to ask fundamental questions, such as: ‘Can we live in a world without central authorities? Can we move value safely without needing to rely on rent-seeking intermediaries that centralise data and thus power? Can DLT provide settlement finality of transactions without the need for intermediaries or legal frameworks such as the Settlement Finality Directive in Europe? Do we still need banks and central banks? Could DLT be the answer to the missing global currency and payment system? Could DLT help digitise the trade and cross-border payments value chain, taking out inefficiencies, fraud and lack of transparency? Could DLT be deployed in a way that would streamline and simplify today’s complex securities trading, clearing, settlement and post-trade processes?’

Inspired by Bitcoin and its underlying blockchain distributed ledger (DL) and driven by the objective of supporting financial stability oriented innovation we investigate how technology innovation combined with regulatory and governance aspects can transform the world of payments, settlement finality and money.

1.2 OUTLINE

This dissertation is composed of three essays that follow the common thread of technology innovation and financial stability in the world of payments and money. Innovation at a broad level can be described across various dimensions, including organisational, technological, societal, social, economic, marketing and other related angles, broadly defined as something that is changing the way we operate. Baregheh et al. (2009) are addressing the absence of a clear definition of innovation by providing a multidisciplinary definition of innovation. In this thesis we focus on technology innovation as applied to the financial services infrastructure space with a particular emphasis on DLT and the context of payments. The objective is to demonstrate that financial stability concerns and the evolving role of financial institutions, infrastructures and central banks can be proactively approached with help of this technology innovation.

We examine payments across both the wholesale and retail space. The wholesale payments space is of particular interest, given the financial stability related risks that should be tackled in order to avoid future crises. At the same time technology innovation and the role of data and transparency can play a key role in making this business safer, more efficient and compliant. The retail payment space, on the other hand, is an area of focus because policy measures in Europe to open up banking and payments combined with new payment solutions could lead to challenges for data security, privacy as well as system stability. These may result in a call for safer, government provided back-up solutions for retail payments.

In the broader context of accelerated technology innovation and competition from non-financial and non-regulated entities and processes in the emerging 'sharing economy', several directions for the financial industry are laid out and implications of these are being discussed.

With regard to research methodology there are several different research approaches used in economic and other experimental research disciplines (Creswell, 2018). For our research we have chosen three different sets of research methods considered to be most appropriate to the themes that are being examined. A combination of theoretical, empirical survey and case study methodological approaches were chosen to bring to light the way in which money and payments are transforming as a consequence of innovation.

In Chapter 2: Proof of Work Blockchains and Settlement Finality: a Functional Interpretation? we aim to provide an interpretation of the legal issue of settlement finality in the context of proof-of-work (PoW) DLT, using the example of Bitcoin. This context is of particular importance as final settlement plays a crucial role in removing settlement risks between counterparties, in support of financial stability. Such risks today are concentrated within and eliminated by - or sufficiently mitigated by - regulated FMIs. In the EU, FMIs achieve final settlement under the Settlement Finality Directive. In contrast, the Bitcoin network postulates to achieve certainty of settlement of its cryptocurrency in a trustless environment without the need for such intermediaries but also without recourse to any legal provisions.

The literature review on settlement and settlement finality shows that research so far reflects the basis of centralised and regulated systems. The PoW blockchain is not a centralised system and, in the same vein, it is not subject to any legal or regulatory frameworks. We identify a gap in the literature as none of the concepts of settlement or settlement finality can actually apply to PoW blockchains. Nevertheless, value transfer does happen in these networks.

For the purpose of expanding research, we extend the earlier work of Berndsen (2013) on functional modelling of the theoretical settlement problem. In terms of methodology, we make a theoretical contribution by analysing the settlement process of PoW with help of Berndsen's model. In order to be able to apply the model to this type of blockchains we first of all modify and expand the model. Subject to these adjustments we find that modelling PoW achieves the result of functional settlement in an immutable way via a distributed settlement process. As a next step we provide a functional interpretation of settlement finality and propose a new encompassing definition of settlement finality for DLs that are based on the PoW consensus algorithm in order to expand the literature on settlement finality.

These findings are of particular interest as they show that settlement finality can be reached in the absence of financial intermediaries such as FMIs, which normally play the settlement entity role. Furthermore, we provide a qualitative assessment of the Bitcoin system versus the legal framework for settlement finality, in order to evaluate whether Bitcoin provides a superior outcome to the backward looking legal regime. This is very relevant in light of growing cyber threats and insider attacks that can occur in relation to FMIs. We find that, subject to a number of caveats and future improvements in DLT and underlying consensus algorithms, this new technology may provide the opportunity to deliver superior results compared to legal frameworks for settlement finality by embedding finality in code.

Chapter 3 – The Future of Correspondent Banking Cross Border Payments – focuses on cross-border correspondent banking payments, a sector that is challenged by regulatory, operational, transparency and capital as well as liquidity related issues. With increased concentration in this market, primarily triggered by regulatory fine risks around AML and CTF compliance deficits, as well as deteriorating underlying economics of this business due to prudential regulatory measures, there is a need to investigate ways to improve cross-border wholesale payments. This research therefore explores whether and how technology innovation, in conjunction with policy measures, can improve this business.

Despite the growing focus by central banks, supranational bodies and regulators on the area of cross-border wholesale payments, primarily driven by the fact that correspondent banking providers began withdrawing services from banks and payment service providers (PSPs) that they deemed to be too risky as a consequence of regulatory fines applied in the AML and CTF context, little attention has been paid to this issue so far by the academic literature, both theoretical and empirical. In addition, the connection between cross-border payments and emerging technologies has not been researched in any depth.

In order to fill this research gap, this Chapter builds on the empirical validation of existing shortcomings in this area. The methodology applied in this Chapter is based on a mixed-method approach that is appropriate for our research question. Our strategy includes a questionnaire, designed to validate our key assumptions as well as the collection of qualitative data via focus group discussions (FGDs). This process allows us to collect and analyse both quantitative and qualitative data. Qualitative data analysis (QDA) is the process of turning written data such as interviews and field notes into findings. Qualitative data is particularly important to understand the impact of particular industry problems and highlight possible solutions.

The first step in our analysis consists of the design of the questionnaire. We carefully designed our questionnaire so as to maximise its usefulness in gathering information. We included close-ended questions. Close-ended questions were in the YES/NO format, but most were based on a Likert scale.

Before sending the questionnaire to respondents, we pre-tested its reliability by submitting it for review to a small number of informed industry colleagues. This step enabled us to verify the consistent interpretation of questions and their validity and effectiveness. Once satisfied with the format of the questionnaire, we opted for an on-line survey, whereby respondents were invited to participate to the survey via email and then to visit a purpose-built webpage to answer the questions. Our aim was to gain a better insight into the way this industry operates and therefore we developed a questionnaire that addresses a number of assumptions that we made in the context of regulatory, operational, technological and efficiency related aspects of correspondent banking. Having empirically identified the key areas of concern (i.e. cost, transparency, speed, compliance), we set up FGDs to evaluate a number of key requirements for the future of cross-border payments.

As a next step the Chapter provides a set of design scenarios for a superior cross-border payment set of processes and network that by their nature will be able to deliver improvements in correspondent banking.

Finally, we outline policy recommendations to complement the technical and organisational future design for cross-border payments, in particular with a view to streamlining conduct, AML/CTF and transparency rules for payment services at a global level.

Chapter 4 – The Future of Digital Retail Payments in Europe: A Role for a Digital Euro? – investigates the changing role of traditional forms of fiat money against the backdrop of the arrival of DLT, private cryptocurrencies and the wave of payments technological and regulatory innovation in the European market. Subsequently, the implications for central banks and their potential role in retail payments are assessed.

Despite the growing literature in this space, the retail payments dimension of Central Bank Digital Currencies (CBDC) or digital fiat currencies has not been researched in any detail. There is a perception that retail payments innovation in Europe is sufficiently dynamic and hence does not necessitate a central bank issued instrument. However, we are filling this research gap with a specific perspective on financial stability, resilience and security, which is becoming more important in the context of the growing data economy. Therefore, this Chapter provides an alternative perspective on the future role of central bank money for the retail sector.

The methodology applied in this Chapter is the case study method, which has been chosen as most appropriate given the nascent space of this research and the particular focus on the transforming role of retail payments in light of technology innovation. We map out a set of potential scenarios based on which we develop a theoretical blueprint that can respond to these.

As retail cash payments move into the digital age with the associated challenges for citizens' data, identity as well as financial stability, the development of a new form of digital fiat currency will become a more relevant consideration for the future of the Eurosystem. A set of scenarios is proposed under which the provision of a digital near substitute of cash for retail payment purposes – a Central Bank Digital Fiat Currency (CBDFC) - which in the context of the EU will be labelled 'Digital Euro', could become important in terms of maintaining financial stability and as well as the link to the citizen.

In a second next step, we propose a theoretical blueprint to the Eurosystem based on which experimentation with a retail payment CBDFC can be explored and tested further. We also highlight a number of open questions and challenges that would need to be addressed and considered before such a new form of central bank money would be introduced in practice.

This research is very timely as central banks around the world are assessing the question of whether they should be issuing a new, technologically innovative form of central bank money in order to both compete with the private cryptocurrency space as well as to support overall innovation, efficiency, financial inclusion and improved monetary policy outcomes for their respective countries.

Chapter 5 summarizes the main findings and develops a set of general conclusions, highlighting practical implications for central banks, regulators and the banking industry. In conclusion we point to the limitations of the studies in order to offer avenues for future research in this rapidly evolving space.

Chapter 2

Proof-of-Work Blockchains and Settlement Finality: a Functional Interpretation?

Disclaimer: This Chapter forms the basis of a paper co-authored with Prof. Ron Berndsen, which has been submitted for publication to 'The Journal of Financial Market Infrastructures'.

2.1 INTRODUCTION

The ability to make a payment with certainty in a legally sound way forms the backbone of transacting in the global economy, in the absence of which commerce would be significantly inhibited. In today's modern economies FMIs play a key role in enabling financial operations (Diehl et al., 2016), ranging from clearing and settlement of payments and other financial transactions or instruments, by centralising these functions and helping to protect participants from financial risks that can arise during transactions; for example in case of insolvency of one or more participants in the system. A famous case that illustrates the consequences when settlement finality is not properly defined or implemented is the failure of Herstatt Bank in 1974, which exemplified foreign exchange intraday settlement risk, or 'Herstatt risk'.

As intermediaries between participants, FMIs also concentrate risk, which is why they have to comply with globally defined principles to ensure that final settlement of transactions is achieved, preferably intraday and as a minimum by the end of the day (Principle 8, CPMI-

IOSCO, 2012). Simply put, settlement finality is reached when the account of the recipient in a payment system has been credited irrevocably and unconditionally. This implies that it is illegal to unwind a transaction that has been settled with finality.

In recent years, the emergence of the Bitcoin blockchain and other DLs, the rise of the 'sharing economy' and the peer-to-peer (P2P) financial services industry (P2P payments, lending, foreign exchange (FX) etc.) initiated a transformation of the financial system. Money as well as the process of payment have evolved and now include crypto technologies. In the future, DLT could be become the *"Internet of Money, connecting finances in the way the Internet of Things (IoT) connects machines"* (Swan, 2015). New models of financial infrastructures and providers are emerging, creating new opportunities but also introducing potential new risks. The central question therefore is whether this innovation is also capable of fulfilling the requirements of settlement finality. In our research we are focusing on DLs with consensus algorithms where there is no central authority at all (i.e. Hyperledger, Corda, Lightning Networks, Ripple etc. are not covered here). In particular we decided to examine the Bitcoin PoW blockchain (Nakamoto, 2008) – a P2P payment system based on the cryptocurrency bitcoin - which was the first one and is thus the most mature example of a blockchain. PoW is one of the few examples where there is really no central authority, up to the point that software needs to be updated as this is done by consensus as well. This distributed and trust-less nature of the Bitcoin blockchain presents a radical departure from the centralised and regulated (thus trusted) clearing and settlement processes of FMIs that have evolved over decades with the main purpose of removing settlement risk in support of financial stability.

Already in 1976 Nobel Prize economist Hayek advocated the use of private currencies in order to achieve currency competition (Hayek, 1976). Even though the Bitcoin system is non-systemically important at the time of writing, assuming that either itself – or a further evolved variant - could be in the future, we want to assess whether Bitcoin by design provides a technologically improved and more efficient alternative to settlement finality in existing FMIs in the payments space. If this were the case, this could have significant implications on the overall design and functioning of the financial system, by removing central risk concentration in FMIs and instead relying on a distributed network for settlement. In this Chapter we do not specifically consider governance or the well-known technical problems of Bitcoin such as scalability.

To address the question of settlement finality in Bitcoin we build on the theoretical framework developed in Berndsen (2013). That framework is designed to be a generic tool that allows for comparisons at a functional level between any type of FMI with a specific focus on studying how different concepts of infrastructure deal with the settlement problem and its solution.

Our results highlight that Bitcoin[1] as an isolated system does achieve final settlement in a functional way, i.e. it is economically unprofitable to unwind a bitcoin transaction. As this is accomplished without the involvement of any financial intermediaries, it begs to consider a new definition of settlement, which we propose in order to fill this gap in literature. We also find that risks, which can arise from a hard 'fork' in the blockchain, do not lead to true credit risk for participants – as demonstrated with the Bitcoin 'hard fork' that took place in August 2017.

---

[1] We will denote the Bitcoin system with a capital, and bitcoins as a currency in lower case. Furthermore, bitcoin is denoted by BTC and the bitcoin cash spin-off by BCH. We will also use the term Bitcoin and PoW blockchain interchangeably in this Chapter.

The consequence of the fork was the creation of two Bitcoin versions, Bitcoin (based on the existing version of the algorithm) and Bitcoin Cash, which operates on a different protocol.[2] The risk of double spending is also mitigated by the Bitcoin PoW consensus protocol itself. However, liquidity risk can arise in case of late or non-executed transactions. This can occur when those get deprioritised due to insufficient fees included in the instruction. Compared to traditional systems, which are able to unwind transactions, where users can legally challenge those, Bitcoin transactions are irrevocable and immutable, providing more certainty for users but no protection in case of erroneous or fraudulent transactions. However, there are escrow type solutions as well as multi-signature solutions, which provide additional security for users, e.g. by holding users' coins in escrow until the conditions of a sale have been fulfilled or creating a multi-signature address - which for example can require both buyer and seller to sign – which is used to send the coins to. Obviously, this reintroduces the need for some trust in an intermediary, the escrow service provider.

This paper is organised as follows. Section 2.2 provides a condensed overview of the Bitcoin network by outlining only relevant elements of Bitcoin that are needed in the context of the settlement question. Section 2.3 reviews the literature on settlement finality. Section 2.4 lays out two distinct Bitcoin scenarios that will be used as the basis to examine settlement finality. Section 2.5 provides an overview of the theoretical model and sets out the research questions of this Chapter. Section 2.6 models the two Bitcoin scenarios in order to analyse and interpret settlement finality.

[2] The Bitcoin 'hard fork' of 1 August 2017 resulted in a chain split, where the newly created Bitcoin Cash shares its entire transaction history with Bitcoin up the point of the split and following that created its own blocks. In practice this meant that users have as many new Bitcoin Cash coins as they have bitcoins before the split and both coin types can be spent independently of each other. Note however that some cryptocurrency wallet providers did not support both cryptocurrencies.

Section 2.7 reviews Bitcoin in light of the global Settlement Finality Principle[3] and legal frameworks based on this principle and provides a view on whether or not the PoW consensus algorithm is superior to the legal basis. Section 2.8 discusses the results and is followed by the overall conclusions in Section 2.9.

[3] Principle 8 (CPMI-IOSCO, 2012): Settlement finality

An FMI should provide clear and certain final settlement, at a minimum by the end of the value date. Where necessary or preferable, an FMI should provide final settlement intraday or in real time.

2.2 CONDENSED OVERVIEW OF THE BITCOIN NETWORK

Nakamoto (2008) postulated a protocol and network for exchanging value that would not rely on financial institutions as trusted third parties but instead be based on cryptographic proof. As such it is aimed at functioning in a completely trust-less world. The problem of creating a workable system in a trust-less environment is a difficult one which previous attempts to create electronic cash systems such as e-gold, Liberty Reserve etc. could not solve. In essence, it relates to two important challenges in distributed computing:

1) the Byzantine Generals Problem (Lamport et al., 1982), which describes the difficulty of ensuring the secure exchange of messages in a network of unknown participants that cannot be trusted; and

2) the Double Spending Problem (Garcia, Hoepman, 2005), which occurs when electronic cash can be spent twice or more times by broadcasting malicious transactions to the network, which has no central authority to check and track transactions and thus cannot validate the correct sequence of transactions.

The solution to these two problems provided in Nakamoto (2008) builds on a particular combination of well-known algorithms for asymmetric cryptography such as SHA-256 (Secure Hash Algorithm) and PoW consensus algorithm Hashcash developed in Back (2002). The key differences and similarities between Bitcoin and traditional payment systems are summarized in Table 2.1

Payment Systems	Bitcoin Blockchain
• Network with a central operating node	• Distributed network
• Account Based	• Cryptographic Keys
• Fiat currency (backed by or in central bank money)	• Private cryptocurrency (not backed)
• System and currency are separate	• System and currency are integrated
• Highly regulated and supervised	• Not regulated and in parts almost impossible to supervise
• Full information/transparency on sender and receiver by central operator	• Pseudonymity, with option to separately combine data to identify individuals
• Batch or single transaction processing	• Batch processing
• Within ledger transfers	• Within ledger transfers
• Multitude of ledgers with no common view and associated complexity, significant reconciliation costs for participants	• One immutable ledger or transaction log, that is shared with all participants and updates automatically

Table 2.1: Comparison of Bitcoin and payment systems

The common structure of a payment system is where a national central bank acts as money issuer, money redeemer and final settlement entity at the centre of the payment network. In Bitcoin a network of nodes runs the Bitcoin protocol to maintain the blockchain. This underlying software protocol is based on a complex consensus process that requires the majority of players to participate (i.e. all full nodes are part of the infrastructure). However, whereas Baran's network model (Baran, 1962) implies that all nodes are equal, in the Bitcoin system this is not the case today as only those computers (nowadays mostly using an Application Specific Integrated Circuit, short ASIC) with significant processing power can provide resources to the network to support transaction verification and confirmation, i.e. mining (Milne, 2017). Furthermore, a few core developers play a key role in updating the protocol, resembling the role of a central bank (Grinberg, 2012), but their influence is ultimately dependent on the majority support of user nodes.

The Bitcoin blockchain is hailed as a technology that allows for the removal of a single point of failure, because of the absence of any centralised entity that could constitute a risk when hacked or technically down. Even if a participant has a hardware failure due to which he loses the chain of blocks represented in the blockchain ledger on his computer, this would only be a temporary problem because an updated ledger can be downloaded again at any time. Only users can be 'hacked' and private keys can be stolen, but there is to date no 'hack' of the blockchain itself.

2.2.1 The Main Building Blocks

In terms of building blocks Bitcoin is effectively composed of three key elements. Firstly, Bitcoin has a token of value in the form of bitcoins, a cryptocurrency, which is used to transact between participants of the network as well as to reward network nodes for their transaction-processing role. Whether bitcoins are formally recognised as currency, depends on the stance of governments and regulators. From the point of view of economic theory, a currency would have to fulfill the three requirements of acting as a store of value, a medium of exchange and a unit of account. Despite the initial focus on the property of medium of exchange, the observed volatility (in particular in 2017-2018) of the bitcoin price appears to de-emphasize the feature of store of value and rather points to bitcoins being treated as an asset. Its practical role as a unit of account is debatable (many decimal places). Bitcoins are minted continuously, subject to a decreasing-supply algorithm (to mimic commodities mining such as gold), whether demand in the market is high or not. Therefore any strong market demand leads to extreme price increases of bitcoins (see www.blockchain.info), whereas prices tend to collapse when market demand is low. This feature of fixed bitcoin supply bears some resemblance to Milton Friedman's k-percent rule (Friedman, 1960), which proposed to fix the annual money supply growth rate.

The crucial difference however is that by around 2140 the overall limit of 21 million of bitcoins[4] will have been mined, which ultimately makes it a deflationary currency. Unlike central banks, which regulate the monetary base and have tools available to steer the supply and value of a currency when required, Bitcoin does not cater for this. As discussed in Böhme et al. (2015), this begs the monetary policy question as to what happens when economies grow at a different rate than money supply.

Secondly, Bitcoin operates an open source based, decentralised public ledger, the blockchain. This DL is a form of accounting that embeds reconciliation and provides both the public history of all transactions ever occurred on the network as well as proof of value or record of ownership of bitcoins. As an append-only database, data can always be added to the ledger but cannot be removed once included. Unlike banking, accounts are decentralised down to the user level.

Thirdly, the Bitcoin model uses a particular form of consensus algorithm called PoW. PoW operates on the basis of mathematical problem solving, which involves non-invertible hash functions (Campell, 2016) based on SHA 256 developed by the National Security Agency (NSA). In practice the mathematical functions are operationally hard to solve – which means that a lot of attempts have to be made (and energy spent) before a solution is found - but once solved, it is computationally easy to check that it is in fact a solution (a decryption has taken place). Network nodes acting as validators or miners select those pending transactions that are in line with the bookkeeping rules of the ledger, i.e. only those Bitcoin addresses, which are available to the sender of the transaction are updated, making it impossible to spend more bitcoins than you own. Every input for a new transaction refers to the output of a previous transaction.

[4] The 21 million limit in 2140 follows from the initial reward of 50 bitcoins and the reward halving period of 210,000 blocks (roughly every four years).

By checking the public cryptographic key of the sender against his private cryptographic key based signature, the network establishes the fact that the sender is the owner of the bitcoins associated with this specific address. This practically means that the sender has unencumbered bitcoins to spend – unspent transaction outputs, UTOX - i.e. the transaction is fully prefunded. Once the PoW solution has been found it is published in a batch ('block') with other transactions to the whole network, appending a new block to the chain. All participants can check that the new block in the chain only includes permissible transactions (no double spent) and that the correct solution to the mathematical challenge has been found. The transaction is non-repudiable and from then on the updated ledger version is used as input to the hash function and hence forms the new basis for validating pending transactions. This immutability is one of the key benefits of the Bitcoin blockchain as it allows an immutable audit trail of every transaction.

At the origin of the whole Bitcoin blockchain is the genesis block (the only valid block without a predecessor, but meeting the requirements of the protocol). Every block in the blockchain must have a so-called coinbase transaction as its first transaction where the input for this transaction can be arbitrary[5] (up to 100 byte in size) and the output is used to send a block reward to the miner that has successfully calculated the PoW. This reward consists of a subsidy – which can be considered as a form of money issuance – plus the transaction fees for all transactions in that block, which are all sent to the successful miner's address.

[5] Note that the Bitcoin genesis block famously contained the following input: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks".

The coinbase thus represents the core of Bitcoin's monetary policy, enabling the creation of 'money', i.e. bitcoins. It halves every four years, which means that by approximately 2030 the reward provided by the coinbase will be lower than the transaction fees – hence by this time fees will become the main form of PoW compensation.

Despite Bitcoin's design features, there is a theoretical possibility for anyone who controls more than 50% of the processing power to perform an attack on the network (this is known as the '51% attack'). The arrival of' 'mining pools', where miners join their CPU forces and share the bitcoin fees and rewards, makes such an attempt possible. However, the sheer fact that such an attack would not only be discoverable but would very likely lead to a devaluation of bitcoins, provides an economic disincentive for anyone capable to effectively mount such an attack. In addition, an attack could only be executed successfully, if the attacker would redo the PoW of the current block as well as all of the subsequent blocks and then surpass the work of the honest nodes in the network. Another system design element that helps prevent this risk is the fact that the difficulty of PoW is determined by a moving average, which targets an average number of six blocks per hour. In case these blocks are generated too fast, compared to the average, the grade of PoW difficulty increases automatically after 2016 blocks, which corresponds to approximately every two weeks.

Following the logic of Moore's Law (Moore, 1965), as computational power evolved, speed increased and hence the in-built functionality to adjust the degree of difficulty of PoW became more important. Researchers have theoretically demonstrated that attacks could affect the system if payments were to be processed at a faster rate than that (Karame et al., 2012).

As we can see from the outlined building blocks, Bitcoin operates as a form of payment messaging network with an embedded native currency or asset, bitcoins, that performs transaction based reconciliation for decentralised user accounts. No central party controls either the network or the currency and no central party issues bitcoins or provides convertibility into other currencies within the system.

2.3 SETTLEMENT FINALITY

The challenge in payments is that transactions between parties generally carry risk. This risk can be broadly defined as settlement risk and comprises a number of risk scenarios that can arise when payments do not settle smoothly. These risks include credit, liquidity, operational and legal risk, where all of these have the potential to trigger systemic risk (Kokkola, 2010). From a central bank perspective the mitigation of settlement risk is a key concern as it supports systemic stability overall. As a consequence CPMI-IOSCO have issued global principles for all FMIs with a view to mitigating these risks (CPMI-IOSCO, 2012).

Despite the importance of the payment system and settlement nexus, the academic discipline of payment economics is still in its infancy. Nosal and Rocheteau (2006) note the absence of a *"well-defined literature on payments"*. Roberds and Kahn determine the field of 'payment economics' as the study of payment systems, which they define as *"any arrangement that enables exchange by overcoming the paired frictions of time mismatch and limited enforcement"* (Kahn, Roberds, 2009).

In their 2002 paper on finality, Kahn and Roberds discuss the nature of 'inside money', i.e. debt (e.g. bank deposits), in the context of payment systems, as the curial basis of exchange, where debt claims (a bill or mortgage payment or even a trading position in the market) can be *"extinguished by the transfer of another (bank deposit)."* (Kahn, Roberds, 2002). They consider that the nature of finality is so essential that without it *"a transfer of bank funds would not necessarily constitute a payment and "money in the bank" would not function as money."* (Kahn, Roberds, 2002).

Source	Definition and Features of finality and settlement
Berndsen (2013)	"…settlement, i.e., legally discharging financial obligations of clients, financial intermediaries or other settlement entities"
BIS (1997)	"…it is typically understood that…final settlement occurs when … transfer of value has been recorded on the books of the central bank."
CPSS-IOSCO (2012)	"Settlement finality occurs when the account of the receiver within the payment system has been credited and settlement is unconditional and irrevocable. "
Kahn & Roberds (2002)	"…This infrastructure determines, amongst other things, the finality of a given transfer – the circumstances under which the transfer of an asset (in practice, almost always a deposit or line of credit with a bank) extinguishes a debt."
Kahn & Roberds (2006a)	"…finality…..A debt transfer is "final" ("the debt is discharged") when the transfer extinguishes an obligation between two parties….The higher the degree of finality, the more money-like the character of a debt transfer."
Kahn & Roberds (2009)	"… "finality". A funds transfer over a public system typically represents an unconditional transfer of a claim on a central bank. As such, it unconditionally discharges an obligation: payment may effectively be thought of as settlement…."
Köppl, Monnet, Temzelides (2006)	"Settlement has three defining properties. It is not a welfare-improving activity by itself. Second, it takes place periodically. Finally, settlement gives the opportunity to all participants in the system to start afresh since, after settling their obligations, they are no longer liable to the system."
ECB (2010)	"A settlement or transfer is final when it is unconditional, enforceable and irrevocable, even in the framework of insolvency proceedings opened against a participant… A distinction should be made between the finality of the transfer order and the finality of the transfer, which indicates the moment at which entitlement to the asset in question is legally transferred to the receiving entity." "Settlement: The completion of a transaction or of processing with the aim of discharging participants' obligations through the transfer of funds and/or securities. A settlement may be final or provisional."
Lawrence (1997)	"Final payment is the moment when the payment may no longer be revoked."

Table 2.2: The concepts of finality and settlement in literature

Scholars, central banks and other supranational bodies have provided various approaches to defining the concepts of settlement and finality of a transaction as listed in Table 2.2.

A common feature of the above statements and definitions of final settlement is the 'unconditional' nature of the transfer, which thus enables 'discharge of obligations' between the parties involved.

As referenced in several definitions of the table, finality of settlement is traditionally underpinned by legally enforceable rules, which can differ across jurisdictions, but commonly aim to achieve the same objective in line with CPMI-IOSCO Principle 8 (see also BIS definition, 1997). For example in Europe the Settlement Finality Directive (98/26/EC) provides the legal framework for settlement finality. In order to discuss settlement finality in a practical yet precise way we adopt the usage of the TARGET2Securities (T2S) Advisory Group (2017) to define the different moments in settlement finality:

SF1: is the moment of entry of the transfer order in the system;

SF2: is the moment of irrevocability of the transfer order;

SF3: is the moment when the transfer is settled with finality.

More general definitions of settlement finality such as Lawrence (1997), which puts emphasis on irrevocability or Köppl et al. (2005), which highlight the three features of asset transfer, periodic frequency of settlement and removal of liabilities between participants following settlement are more akin to how Bitcoin works. The 'unconditional' nature of settlement, highlighted across several definitions, is of particular interest as we may be able to draw a parallel to the immutability of the Bitcoin blockchain.

To what extend final settlement can happen, depends on the payment system type and design, which developed significantly over the last decades with technological change, settlement risk management, harmonisation as well as speed of transaction being key drivers for transformation. Examples of significant innovation in the European retail payment space include the Single Euro Payments Area (SEPA) initiative (Wandhöfer, 2010) and the arrival of instant retail payment settlement such as the ECB's Target Instant Payments Settlement (TIPS) service.

Today 18 countries have live retail real time payment systems in place[6] and a further 10 countries, plus the SEPA area are considering or in the process of building or launching such systems.[7] In parallel, the wholesale payment space has moved from deferred net settlement systems (DNS) to real time gross settlement systems (RTGS) and Payment versus Payment (PvP) Settlement. These developments go hand in hand with increased regulatory and supervisory scrutiny to ensure that settlement, operational and counterparty risks as well as compliance with know-your-customer (KYC), AML and CTF rules can be managed.

Academic research has analysed the evolution of systems, see Angelini (1998), McAndrews and Trundle (2001), Kahn and Roberts (2001; 2003), Lester et al. (2005). Several scholars have concentrated on developing frameworks or models that would permit the analysis and comparison of payment systems, e.g., Kahn and Roberds (2009), Holthausen and Rønde (2000), Köppl et al. (2006) and Berndsen (2013).

In relation to cryptocurrencies and DLT we begin to see some scholarly papers that start to examine different aspects of this new payment phenomenon, which since then has paved the way for more than 1000 cryptocurrencies (so-called altcoins) and tokens (however Bitcoin remaining the largest by far). Central Banks, regulators and supranational bodies have all developed opinions and research on cryptocurrencies and the potential implications for the payments market.

---

[6] Countries with existing systems include: Sweden, Norway, Denmark, Iceland, UK, Poland, Switzerland, Nigeria, South Africa, China, India, Mexico, Chile, Brazil, Hong Kong, Singapore, Japan and South Korea.

[7] Countries planning or building retail real time payment systems: US, Canada, Columbia, Australia, Thailand, Indonesia, New Zealand, Turkey, the SEPA area, Sri Lanka and Malaysia.

The European Central Bank (ECB, 2012, 2015), the Bank of England (BoE, 2014 a, b), the Bank for International Settlements (BIS, 2017), the BIS Committee on Payment Infrastructures (CPMI, 2015, 2018), the IMF (IMF 2016) as well as regulators such as the European Banking Authority (EBA, 2014) and the European Parliament (EP, 2016, 2017) have all written about cryptocurrencies, examining how these operate, where challenges are seen for users and regulators as well as discussing potential applications across financial services and the future role for central bank issued forms of digital or cryptocurrencies – for the latter see Chapter 4 of this thesis. Bitcoin, in particular is discussed by scholars such as Peters et al. (2015), Böhme et al. (2015) and many others.

Barrdear and Kumhof (2016) argue in their research on the economics of CBDC that the central problem of existing private types of cryptocurrencies, such as Bitcoin, does not lie in the viability of the DL but rather in the level of cost that arises from the verification process. This cost however is necessarily linked to the trustless nature of private cryptocurrencies and can be removed as soon as a trusted environment is being established. Kumhof and Noone (2018) further explore the potential balance sheet implications of CBDC under three model economies and discuss core principles that could mitigate the risk of a digital bank run in those circumstances.

The literature review highlights that in relation to DLT and Bitcoin innovations there are still gaps in our understanding. We have well-established literature for the different approaches to settlement in the traditional, highly centralised world of FMIs. But we find that the definition of settlement here is not appropriate for distributed, intermediary and regulation-free systems such as PoW blockchains.

2.4 MODELLING SCENARIOS

To examine whether there is settlement in Bitcoin we will look at two distinct scenarios. This two-step approach is important in order to understand the original intent and early phase of operation of Bitcoin compared to how this process has inserted itself into the broader financial ecosystem as a consequence of increased mainstream usage.

2.4.1 The 'Pure Bitcoin' Scenario

The first scenario, which we will call Bitcoin 'Pure Bitcoin', reflects the early days of Bitcoin, where only a few coders/miners were part of the system, and all of them were acting as full nodes. This was the time when no connections had yet been established to the outside world, i.e. the only way bitcoins could be obtained was through mining and subsequent exchange of bitcoins between participants.

2.4.2 The 'Bitcoin Ecosystem' Scenario

This second scenario extends the 'Pure Bitcoin' scenario by adding providers and functionality within the system as well as external providers and services, which allow users to bridge government-issued fiat currency and private cryptocurrency. Because of the increased complexity of this more mature Bitcoin environment, we have various types of transactions, some happening sequentially and some simultaneously, with some taking place within the Bitcoin system and some outside of it. This means that we have different layers of settlement risk exposures.

2.5 THEORETICAL MODEL AND RESEARCH QUESTIONS

Our theoretical model basis, taken from Berndsen (2013), is the Uniform Functional Model of the financial infrastructure, or in short UFM. The model, which is based on graph theory, has been designed to assess and compare 'any' type of infrastructure in the financial market space. However the original model was developed before cryptocurrencies became *en vogue*. Therefore, in order to test that the model is indeed uniform, we have chosen to apply it to Bitcoin. If the model is robust, it should be usable as a theoretical tool to examine the settlement problem and solution in Bitcoin.

2.5.1 Introduction to the Uniform Functional Model of the Financial Infrastructure

The UFM covers three key domains: the settlement risk exposure, the value space (i.e. value moving across settlement accounts) and information messages. The model also introduces three types of agents: the client, the financial intermediary and the settlement entity, which display different relationships between each other across the settlement risk, messaging and settlement account space. The roles of these agents reflect the end-to-end lifecycle, i.e. the client creates the settlement risk exposure, the financial intermediary modifies or adds to the settlement exposure risk and the settlement entity concentrates these risks with a view to removing the settlement risk exposure. Note that this set up assumes that agents are acting under 'normal behaviour'. The UFM also allows for multirole agents, i.e. agents that may act in more than one capacity, but can only do so once at a time and not simultaneously. Any multirole agent acting in a higher-level role may also act in lower level roles (but not the other way around).

The roles and relationships of agents across these three domains are visualised with help of the settlement risk exposure graph, the settlement account graph and the instruction lifecycle graph (see Berndsen, 2013).

The following key definitions underpin the overall model:

1) *Transactions (i.e. creating settlement risk exposure);*
2) *Basic elements such as the notion of settlement accounts (for safekeeping the value) and information messages (structured formats based on a pre-defined library of message types);*
3) *Solving the settlement problem by having a necessary condition for settlement (finality) but also a sufficient condition for settlement as the counterparties in the transaction need to be notified (awareness). If both conditions are met, the settlement risk exposure is extinguished.*

2.5.2 Research Questions – Part 1

In step one of this Chapter (Section 2.6) we examine the following two research questions applying the UFM to Bitcoin as follows:

1: "To what extent is the UFM framework capable of defining settlement finality in the 'Pure Bitcoin' scenario? "

2: "To what extent and under which conditions is the UFM capable of defining settlement finality in the 'Bitcoin Ecosystem' scenario?"

The reason why settlement finality in Bitcoin is not straightforward is the occurrence of so-called 'forks'. There are three types of forks:

1) **Chain fork** (Fc): A chain fork is part of the PoW protocol and it occurs frequently in the Bitcoin network when two miners each find a block almost simultaneously. While ultimately the branch with the highest amount of work done (usually the longest chain) 'wins', during the time-interval when a fork exists there is uncertainty about the status of the transactions in both branches. There is an economic incentive for miners to continue working on the longest chain, which means that these forks are usually only one block long and considered as normal statistical loss (from a miner's perspective because the coinbase reward will not be collected). These blocks are also called 'orphaned blocks'. A transaction that ends up in an orphaned block is not confirmed and returned to the memory pool, which is the place where transactions that have not yet made it into a block, are stored (comparable to a payment queue). In case a transaction is purged from the memory pool, it can be considered as if the transaction had never occurred in the first place. Therefore funds are not lost but instead the transaction is not executed, similar to a payment return process in classical payment systems. In general, all orphaned blocks have been forked at some point in time. Figure 2.1 shows the number of transactions in the memory pool between May 2016 and August 2018. It is noteworthy that the numbers were highest at times when the bitcoin price was starting to significantly increase – e.g. April - May 2017 and October - December 2017 (see for example www.blockchain.com for Bitcoin price statistics). This shows that once demand increases significantly, processing in the system becomes a challenge due to limited scale capacity and high latency.

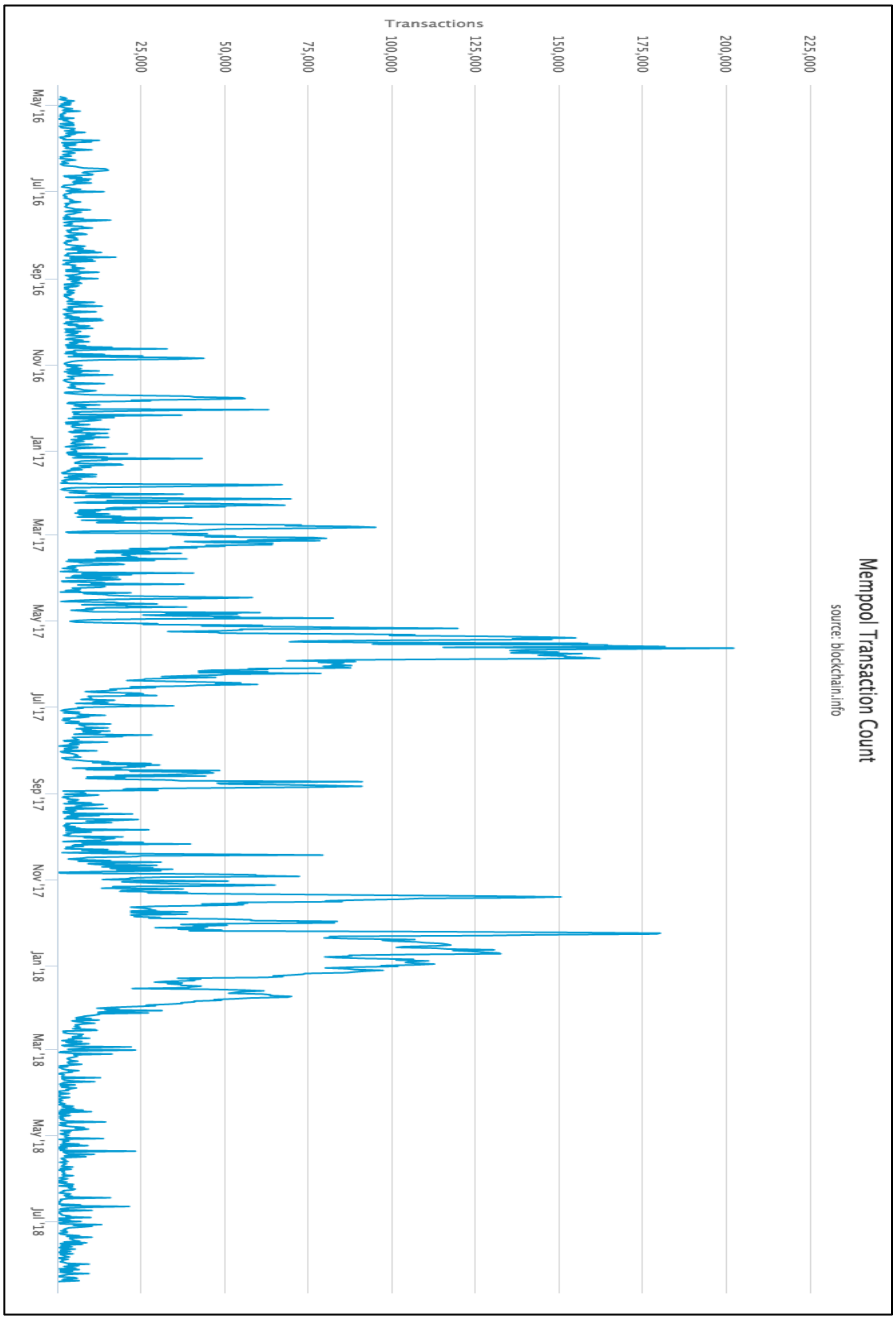


Figure 2.1 Bitcoin Memory Pool transactions May 2016 – August 2018

(source: www.blockchain.com)

2) **Soft fork** (F_s): A soft fork is the result of a change in the protocol which is such that the new protocol accepts blocks valid under the old protocol (backward compatibility) but also accepts blocks that were not valid previously. The soft fork is usually pre-announced to take place at some future, predefined height of the blockchain. Soft forks occur for example with the release of a new version of the bitcoin software.

3) **Hard fork** (F_h): A hard fork is the result of a change in the protocol which is such that the new protocol no longer accepts blocks valid under the old protocol but only accepts blocks that were not valid previously and are consistent with the new protocol. In this case the existing blockchain is copied from the genesis block up to and including the block after which the hard fork takes place.

2.5.3 Research Questions – Part 2

As a second step of this Chapter (Section 2.7), we will test whether Bitcoin PoW can be interpreted in light of the three steps of settlement finality (mentioned in Section 2.3). Against this background we will assess the following research question:

3. "With a view to limiting unwinding and systemic risk, to what extent can Bitcoin PoW achieve a qualitatively better outcome compared to the legal principle of settlement finality?"

2.6 MODELLING THE BITCOIN SYSTEM

This section will apply the two distinct Bitcoin scenarios under the UFM and in doing so, sets out where changes or enhancements to the theoretical model will have to be made as well as interprets if and how final settlement is being achieved in the system.

2.6.1 Modelling 'Pure Bitcoin'

In relation to the definition of 'transaction' in the UFM, i.e. "an implicit or explicit contract between two clients...concluded at time t_T (trade date) consisting of two legs l_1 and l_2..." (Berndsen, 2013) we will have to consider that the coinbase is a type of transaction that does not neatly fit into this definition, because it is not linked to any specific contract (or payment agreement) that is concluded on a trade date. However, it is part of an embedded transaction validation process in code. The reason for this is that the UFM was focussed on settlement but was not intended for the creation or issuance of money. In a coinbase transaction settlement exposure risk is absent on the outset, i.e. no settlement risk arises between miner and network in the first place and thus the coinbase is not playing a role in solving the settlement problem. We will therefore not include the coinbase in the settlement exposure graph but reflect it in the information flow of the instruction life cycle and in the settlement account graph.

With regard to the definition of 'settlement risk exposure' Bitcoin is a system that entails one-sided settlement risk, because we only have a one-way transaction (i.e. there is no exchange between e.g. bitcoins and securities, which would be a two-sided transaction). Therefore we have no visibility as to whether there could be replacement cost risk arising on the other end. We effectively have a case of clean payment, rather than Delivery versus Payment (DvP) or Payment versus Payment (PvP).

A payee in Bitcoin will have ex ante settlement risk exposure, because there is always a risk that a transaction does not get confirmed into a block at all, i.e. that the transaction has not been accepted by the rest of the network (see point on chain fork above). This could lead to liquidity and ultimately principal risk for the receiving party, which could even trigger systemic risk down the chain if transactions were to be sizeable. At the same time opportunity costs would arise on the part of the sender (i.e. tied up liquidity for no benefit in return).

There are four main reasons for unconfirmed transactions:

1) Insufficient transaction fee

In this case miners may have less of an incentive to perform PoW. Both payer and payee would be uncertain in terms of intended versus actual settlement date, versus no settlement at all, i.e. principal and/or liquidity risk could occur. There are various ways to achieve transaction confirmation by inserting a higher fee, either before or after sending a transaction.[8] At a general level it is always possible to wait until either the transaction is eventually confirmed or reappears in the user's wallet – note here that bitcoins actually never leave the wallet until confirmed even though the wallet user interface may indicate otherwise.

From Figure 2.2 it becomes clear that in periods of significant increases in the Bitcoin price, here November 2017 – January 2018, transactions with a low fee attached took several days or longer to get confirmed (for Bitcoin prices, see for example www.blockchain.com).

[8] Some wallets allow for a manual adjustment of the transaction fee, including switching to a 'high priority' service, if the user would like his transaction to be part of the next block. For transactions that have already been sent there are options such as Opt-In Replace-by-Fee (Opt-In RBF), which allow a transaction to be resubmitted with a higher fee (note that not all miners and only a few wallets support this). It is also possible to initiate the original transaction with a higher fee – a "full replace-by-fee", which is accepted by some miners but currently not supported by publicly available wallets.

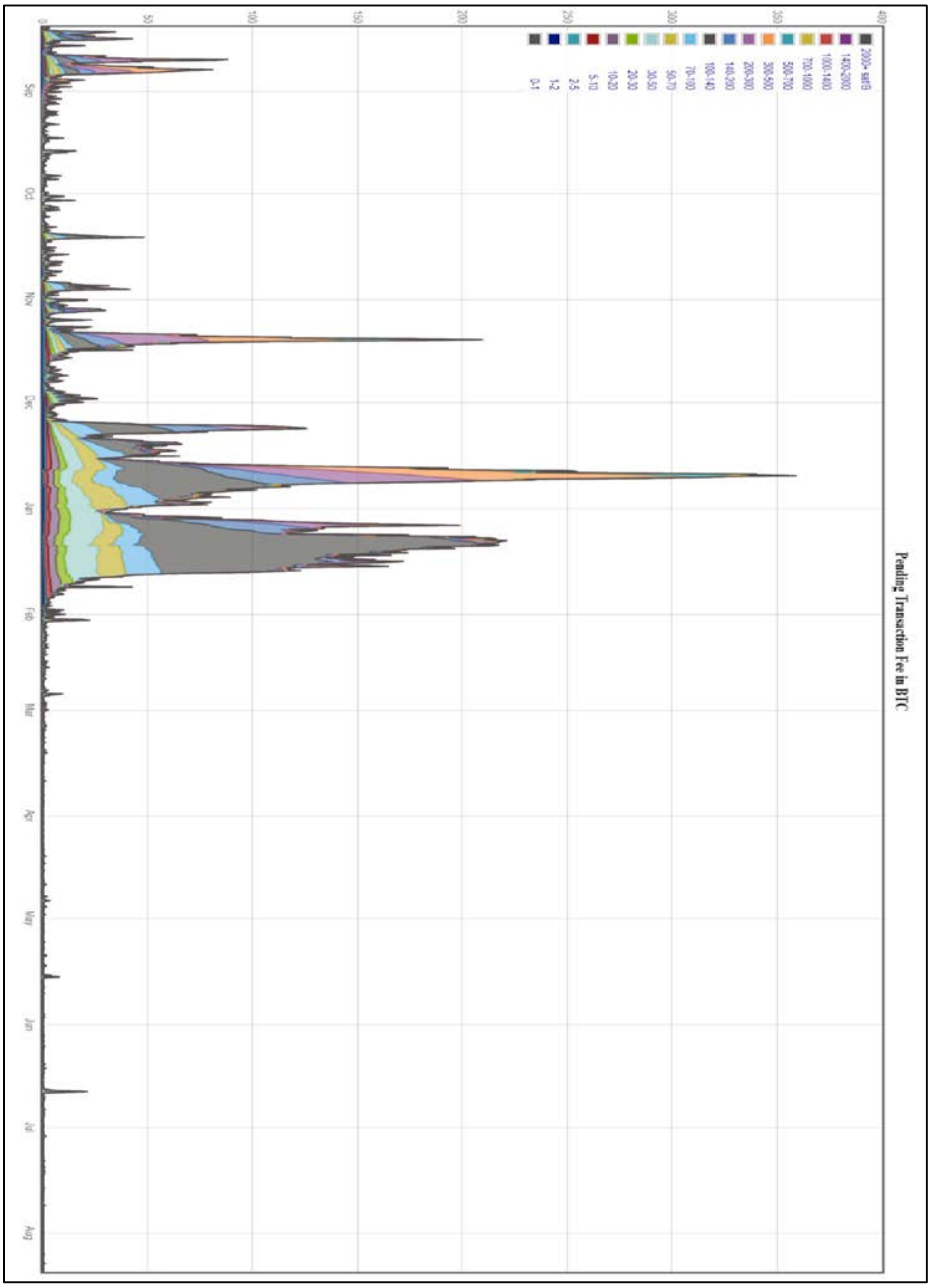


Figure 2.2: Pending Transactions due to insufficient fees August 2017 – August 2018

(Source: https://jochen-hoenicke.de/queue/#0,1y)

2) Double-spend of the same coins

This is only a theoretical risk as explained above. If two transactions are trying to spend the same coins at the same time, one of the two will never be confirmed.

3) Trying to spend unconfirmed coins

For transactions that are still pending, any attempt to try to spend those coins will not be possible in practice. Most wallets wait for a minimum of six subsequent blocks to confirm a transaction and thus to release the coins for the user to spend them.

4) High network volume

This can happen when the amount of transaction requests in the network exceeds the space available in each new block.

The 'Pure Bitcoin' scenario, for the purpose of simplification, will only have three network participants, which are all full nodes capable of verifying all transactions and acting at times as client and at times as settlement entity (i.e. multirole agents). This means that the UFM role of financial intermediary is not required. The definition of settlement entity in the UFM, which is limited to the act of "[*eliminating*] *settlement risk exposure by settling financial obligations of clients or financial intermediaries in its books (book-entry transfer)*" (Berndsen, 2013) will need to be interpreted in a broader sense. In addition to the absence of a legal framework for settlement as well as the caveats mentioned above (de-prioritisation, fork), the settlement process itself is very different compared to the classical FMI processes.

The technology ensures that all nodes are running 'the book', or ledger, at the same time in a distributed fashion. Therefore, a miner solving the PoW can be considered as a settlement entity, but equally the network of the majority of nodes plays a role in the settlement process. Because of this 'joint book-running' process we have one settlement entity, which at times acts as a collective (the nodes) and at times acts as a single entity (the miner). We will therefore denote the set of full Bitcoin nodes as *Settlement Network*, or SN. A single node, which can act as multirole agent in the capacity of settlement entity (either as validator or miner) or client, is labelled as S_i.

An area where UFM will need to be amended is the definition of settlement finality. In Berndsen (2013) settlement finality is defined as representing the act of *"legally discharging financial obligations of clients, financial intermediaries or other settlement entities (but not itself)"* and settlement occurs *"only in those circumstances where the legal ownership changes from one party to another party."* (Berndsen, 2013). In order to capture the concept of settlement finality with respect to Bitcoin we propose to introduce the functional (rather than legal) concept of 'degree of settlement finality (DSF)'. The degree of settlement finality of block *b* at time *t,* denoted by $DSF(b)_t$ in a blockchain is defined as follows:

$$DSF(b)_t = b_t^* - b \qquad (1)$$

where b_t^* is the number of the block with the longest chain from the genesis block and *b* is the number of the block for which we want to determine the degree of settlement finality. DSF $(b)_t$ increases over time starting at zero (if b is the last mined block). DSF is a function of the maximum length of the blockchain and the block number of block b. The maximum is not restricted as the number of blocks in the blockchain is unrestricted as well.

This definition of settlement finality more appropriately reflects the fact that the longer the participants in the system consider the transaction to be settled, the less likely it is that the transaction will be reversed, i.e. transactions that are nearer to the genesis block have a higher degree of finality compared to more recent transaction blocks. In Nakamoto (2008) it is shown that the probability of an attacker catching up via an alternative branch declines exponentially with the number of blocks that he is behind. The practice in the bitcoin community is that transactions embedded in a block six steps deep (this correspondents in the original blockchain protocol on average to an hour) is considered safe. Note that it doesn't matter if there is a chain fork going on at the time of establishing DSF for a certain block as both blocks will temporarily have the same number before one of them is orphaned.

It also important to clarify what we mean by the term 'value' in the Bitcoin world. The UFM defines value as fiat money or the market value of securities, where digital/electronic representations of such values are common these days. To be truly uniform, the concept of value will need to be expanded as bitcoins are neither fiat money nor 'classical' securities, but a private cryptocurrency.[9]

The UFM's concept of value in relation to settlement – i.e. a claim on the issuer, which can only be owned by a client or financial intermediary but not a settlement entity - will have to be considered in light of mining activity. A successful miner, acting as a settlement entity, receives the coinbase as a reward. We will therefore consider that the miner receiving the coinbase acts in the role of a client, rather than settlement entity. The determination that a settlement entity can hold an account with itself, as defined under the UFM, is therefore a usefully broad approach that can be applied in Bitcoin.

[9] Note that this term is not a formal, legally defined term as jurisdictions around the world are taking a fragmented approach to categorising cryptocurrencies.

The open message library approach of the UFM, supporting the exchange and settlement of value, allows for the creation of new types of messages, as required. Messages used in Bitcoin are different to the classical credit and debit messages of the UFM. To fit with Bitcoin, we propose to include the following additional message types to allow for the creation and verification of new blocks and the creation of new bitcoins as follows:

Message ID: GNB = generate new block [blockchain network, current length of blockchain, [list of new transfer orders]]

Message ID: VNB = verify new block [length of blockchain including the new block, blockchain network, successful miner, [list of included transfer orders]]

Message ID: MR = mining reward [successful miner, reward, transaction fee] (i.e. issuance of new bitcoins)

An area that is less straightforward is the definition of 'settlement account'. Under the UFM this type of account is administered by the settlement entity and owned by the client, displaying a legally owned balance, which can change by virtue of the settlement entity applying debits or credits to it (Berndsen, 2013). In Bitcoin there are no accounts in that sense. Rather ownership is reflected by virtue of access to public and corresponding private cryptographic key pairs associated with specific underlying amounts of bitcoins. A transfer of a public/private key pair is commensurate with the transfer of the underlying value of bitcoins. Therefore 'accounts' in the more abstract sense are held at the level of the client. Whether the amounts of bitcoins are 'legally owned' is another question and unlikely to hold in some instances (e.g. where bitcoins are used to launder money); however, the same would apply to fiat currency, where money laundering is prevalent today and very difficult to trace and identify.

In continuation of this argument the UFM's 'necessary condition of settlement of the exposure' should be seen as the change of ownership of bitcoins, within the intended settlement timeframe, as reflected by the applicable DSF. By virtue of having a DL, the 'sufficient condition for settlement' is already implicitly fulfilled, because settlement is a collective process and every node has access to the information on the ledger.

Based on the current level of 'soft forks' we can say that the 'solution of the settlement problem' is completed once a transaction is in a block with DSF ≥ 6, i.e. a transaction that is included in the blockchain six blocks deep can be considered finally validated or settled. This means that in terms of the UFM, ex post settlement risk exposures of previous transactions can be considered dissolved once these are published on the blockchain six blocks ago,[10] the point in time when current Bitcoin market practice would consider a transaction as 'confirmed'.[11]

2.6.2 Example of a 'Pure Bitcoin' scenario application

In this section we demonstrate the application of Bitcoin to the UFM in a concrete example. We have in total three full nodes, S_1, S_2 and S_3, representing three multirole agents acting as client or settlement entity. One full node, S_2, is making a payment of 40 bitcoins to another full node, S_1. Assume for the remainder of this Chapter that the fee equals 1 bitcoin. In Figures 2.3 through 2.5 we show the relevant three types of graphs.

[10] Note that according to the bitcoin protocol the newly issued bitcoins in the coinbase transaction can only be spend after 100 blocks or approximately 16 hours and 40 minutes.

[11] We will not discuss the various bug related incidents that happened with Bitcoin, e.g. the 'Value Overflow Incident', which led to the temporary creation of more than 184 bn. BTC, which then got reversed via a soft fork change to the consensus rules.

Figure 2.3: Settlement risk exposure graph before and after settlement

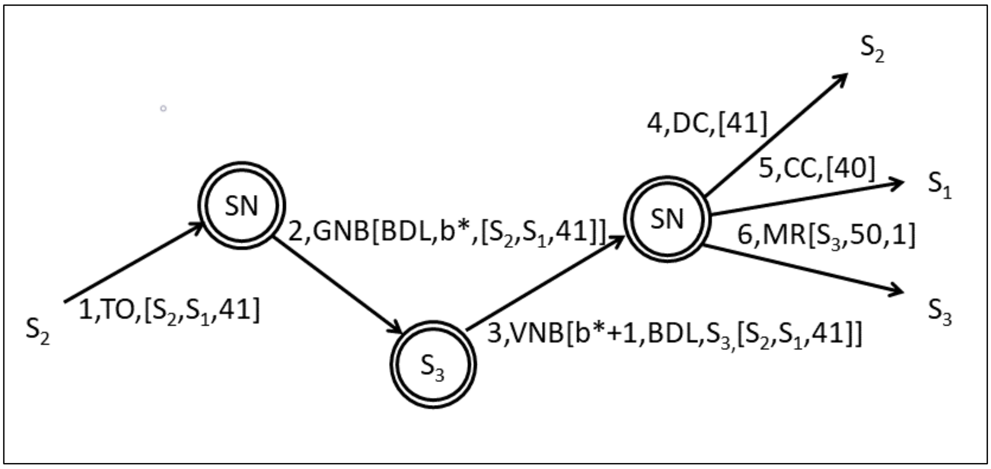


Figure 2.4: Instruction life cycle graph

At the beginning (t_0) S_1 has a settlement exposure in relation to S_2 for the amount of 40 bitcoins (Figure 2.3, left panel). The timeframe for this exposure is between timestamp zero, the point in time when the transaction request is forwarded by S_2 to the network nodes and timestamp *x* (Figure 2.3, right panel), when functional settlement finality is reached (the necessary condition is satisfied) i.e. DSF = 6.

So the intended settlement time for this to be completed is currently (as of 2019) six blocks, which corresponds to 1 hour.

The DSF increases as more blocks are published. At t_x the settlement risk exposure is dissolved.

The instruction life cycle graph (Figure 2.4) starts with S_2 publishing its request (the order to transfer 40 BTC from S_2 to S_1 with a fee of 1 BTC) to the network SN, which contains in our example the blockchain distributed ledger (denoted by BDL). In step 2 the full network, designated by SN, is in charge of generating a new block (GNB) with b* as predecessor block and including the transfer of 40 BTC from S_2 to S_1 and 1 BTC fee. In step 3 a miner (which is neither the sending nor receiving transaction node in this example), S_3, is performing successful PoW, finds block b*+1 and broadcasts the result to the network. The network subsequently provides consensus to this result, leading to the publication of the next block. We call this step 'Validation of New Block'. The newly published block serves as a debit and credit confirmation (note this is a non-legally enforceable confirmation, due to the absence of a legal settlement finality framework) for sender S_2 and receiver S_1 respectively as well as a confirmation of the mining reward (coinbase) for miner S_3 (currently 50 BTC newly issued).

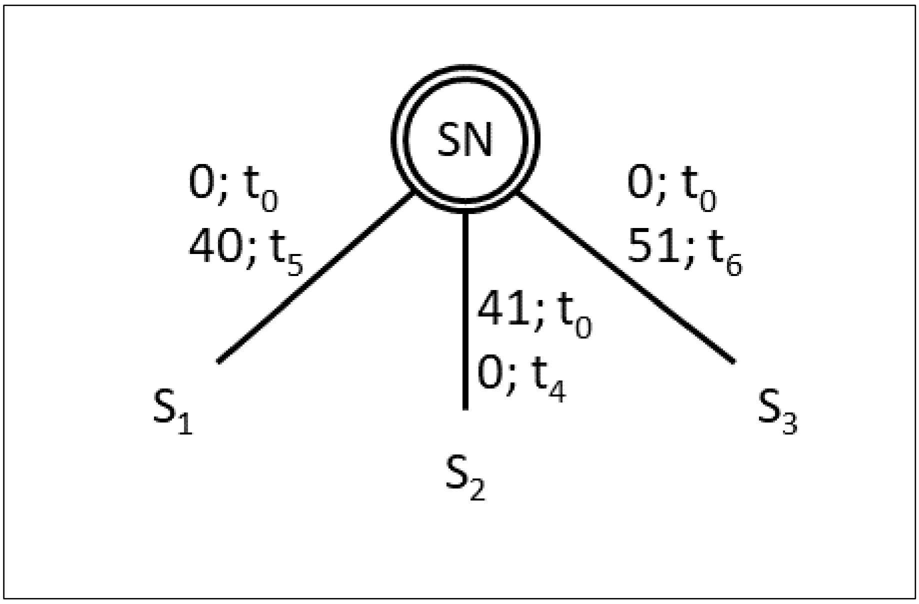


Figure 2.5: *Settlement account graph*

The settlement account graph (Figure 2.5) shows the collective settlement network as SN, which consists of all three nodes. In terms of 'who owns what', the graph shows that 40 bitcoins moved from S_2 to S_1. The miner in the role of client, S_3, receives the mining reward (coinbase), which includes 50 bitcoins reward for performing PoW and an additional 1 bitcoin transaction fee. The timestamps reflect the steps of the Instruction Life Cycle (4 through to 6).

2.6.3 Modelling the 'Bitcoin Ecosystem'

Most of the 'mainstream' users of Bitcoin today may not want to or are not technically capable of engaging in activities of full nodes, such as mining. As an alternative to the traditional full Bitcoin protocol, where users need to download the entire blockchain (>200 GB as of February 2019), we now also have 'lightweight wallets' that provide a user interface comparable to that of an online bank. The lightweight wallet, or Simplified Payment Verification (SPV) protocol, is not able to verify all transactions in a block but only those that relate to the wallet user's activity. This means that they are less secure and rely on other full nodes for validation of the entire blockchain.

With regard to the UFM agents we will therefore need all three types: the client, the financial intermediary and the settlement entity. The lightweight wallet can be considered as a financial intermediary, given its role as enabler of connectivity between client and system as well as messaging and storage of data related to the user's bitcoins. Crucially the lightweight wallet is not part of the settlement network and does not engage in mining.

A further consequence of this set up for users is that they now only have the option of obtaining bitcoins in two ways: receiving them from other users as payment or changing their own fiat currency into bitcoins.

For the latter purpose, the services of so-called Cryptocurrency Exchanges, payment processors that play the role of FX providers for conversion of fiat currencies into bitcoins (and other cryptocurrencies) and vice versa, come into play. In order for customers and merchants to be able to use bitcoins for payment, additional payment protocols, such as the broadly accepted BIP70[12], have also emerged and are supported by most wallet software providers and major payment processors. Research has found that this particular protocol is subject to various cyber-attacks (McCorry et al., 2015). In addition, wallets, depending on their level of security, can be technically hacked and bitcoins stolen. Cryptocurrency Exchanges themselves have been the centre of fraud, e.g. in the case of Mt. Gox, an exchange in Japan, which lost approximately 600,000 bitcoins of its users valued at the time at $188 million and had to file for bankruptcy in 2014. Gadal et al. (2018) also find that during the time of the fraud suspicious trading activity took place, which likely resulted in an unprecedented increase in the USD-BTC exchange rate towards the end of 2013, where the rate moved from $125 in November 2013 to $946 in December 2013 (see www.coindesk.com). Other frauds such as the Bitfinex attack where 120,000 BTC were stolen in 2016, were to follow.

These examples demonstrate that vulnerabilities exist by virtue of connecting to the external environment of new players and business models that are not (yet) regulated in most of the jurisdictions.

[12] The BIP70 is a Bitcoin Improvement Proposal related to a payment protocol enabling communication between customer and merchant in relation to the use of Bitcoin as a payment instrument. The payment protocol consists of three messages: PaymentRequest, Payment, and PaymentACK (acknowledgement), which are exchanged between the customer's and the merchant's server. These messages are ancillary to the Bitcoin protocol and system.

The other definitions of the UFM apply with the suggested modifications and expansions in the same way as described in Section 2.6.1.

2.6.4 Example of Bitcoin Ecosystem model application

Our scenario example for the 'Bitcoin Ecosystem' will be as follows. A customer, c_2, makes a purchase over the Internet and wants to pay the merchant, c_1, in bitcoins. Both payer and payee have a bitcoin lightweight wallet I_2 respectively I_1. These wallets are a form of financial intermediary and thus neither payer nor payee are acting as a full node or miner. The agreed bitcoin purchase price is 40 bitcoins. For each intra-Bitcoin transaction an additional transaction fee of 1 bitcoin will have to be included.

The payer c_2, located in the US, currently has no bitcoins in his wallet and will require the services of a Cryptocurrency Exchange. On the receiving side the payee, merchant c_1, is located in the UK and intends to convert any bitcoins received into GBP. Because of the need for both payer and payee to involve fiat currencies, in addition to bitcoins, we are looking at a set of five transactions that are required in order for the payee to be paid. The three associated graphs for step 2 are depicted in Figures 2.6 through to 2.8. The five transactions are constructed as follows:

<u>Step 1:</u> The first transaction that will have to occur is for c_2 to make a classical interbank credit transfer to a Cryptocurrency Exchange (in our example a US domestic payment). He will send a dollar amount equivalent to the required bitcoins (42 bitcoins) to the exchange, such that the exchange will provide him with 41 bitcoins plus 1 bitcoin (required as fee). Berndsen has already modelled the example of a domestic interbank credit transfer; see Figure 4 of the UFM, page 96 (Berndsen, 2013).

Under the assumption that c_2 holds his regular bank account with a different bank than the Cryptocurrency Exchange, where the exchange will be denoted as S_x, a third settlement entity, such as a central bank, is in charge of settling the interbank exposure (between the banks of c_2 and S_x), as reflected in the settlement account graph. The instruction life cycle and the settlement risk exposure of this step are not shown here but will behave as modelled by Berndsen (2013). Whereas the first transaction step results in the removal of settlement risk for the USD fiat currency transaction, the end-to-end settlement risk has not yet been removed as c_2 continues to be exposed to S_x for the delivery of 42 bitcoins (see Figure 2.6). Assuming that bitcoins in this context are considered as currency, this risk would be akin to classical FX settlement risk. Cryptocurrency Exchanges do not participate in FX settlement risk mitigating processes that would involve regulated systems such as the Continuous Linked Settlement System (CLS), even though CLS is only used for a part of the international market's FX transactions.

Step 2: The second transaction step is a Bitcoin transaction of 42 bitcoins, 41 bitcoins will move from the Cryptocurrency Exchange S_x to the lightweight wallet I_2 of the payer c_2 and 1 bitcoin of transaction fee will move from S_x to the successful miner in addition to the mining reward. The settlement risk exposure of this transaction, effectively a Bitcoin Closed-Loop payment, is shown in Figure 2.6: c_2 has acquired a settlement risk exposure on S_x at time *i* for the amount of 42 bitcoins which is eliminated at *i*+9. Note that the original settlement risk exposure between c_1 and c_2 on the left in Figure 2.6 still exists after step 2.

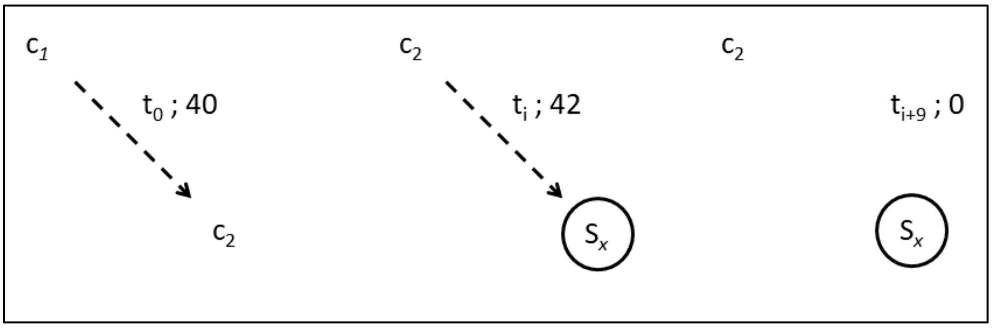


Figure 2.6: Settlement risk exposure graph after step 2

The timeframe for this exposure is between timestamp *i*, the point in time when the transaction request is forwarded by S_x to the network nodes and timestamp *i*+9, when functional settlement is reached (i.e. the necessary condition is satisfied). The intended settlement time for this to be completed is when DSF = 6.

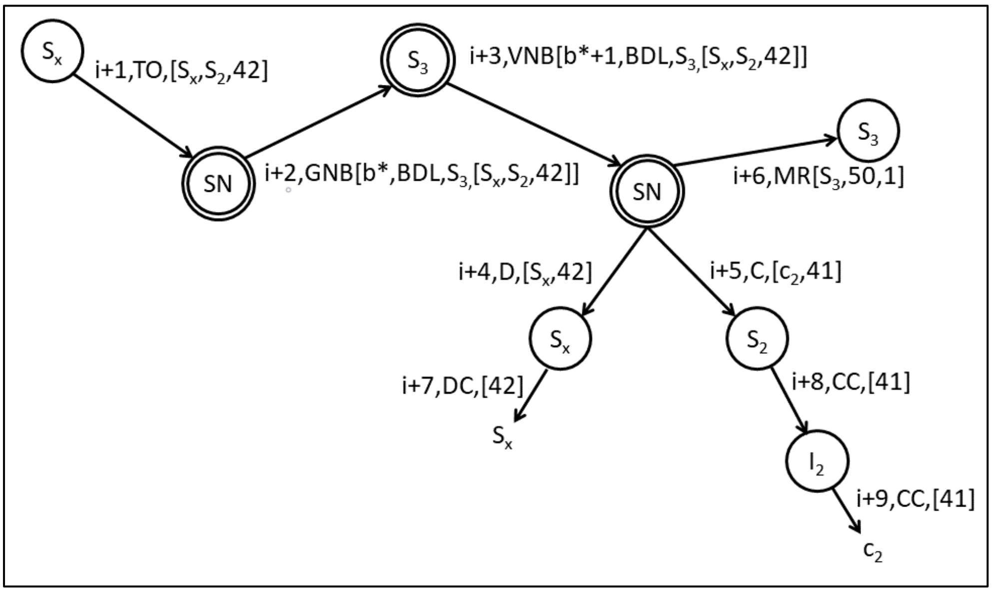


Figure 2.7: Instruction lifecycle graph of step 2

In comparison to the 'Pure Bitcoin' scenario we can see that complexity within the Bitcoin system has increased. In the instruction life cycle graph of step 2 (Figure 2.7) we now have a lightweight wallet I_2 of client c_2 and the exchange (node S_x) which act as financial intermediaries, supporting the communication of the payment instruction and payment credit and debit confirmations on behalf of sending and receiving clients. The successful miner is again S_3 in Figure 2.7.

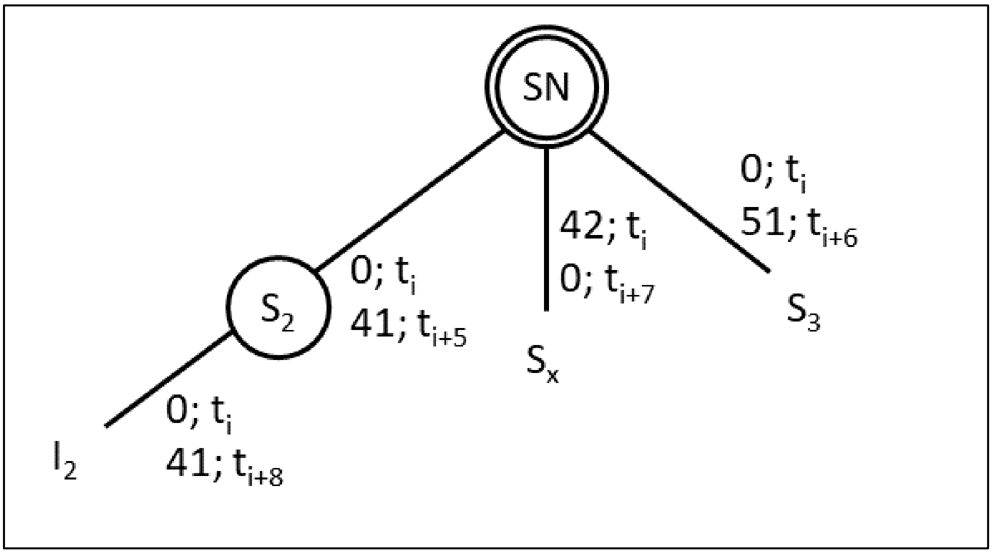


Figure 2.8: Settlement account graph after step 2

The settlement account graph (Figure 2.8) shows the status of the collective settlement network SN after step 2. S_3 as the successful miner receives his mining reward MR for performing the PoW (the coinbase plus 1 bitcoin additional fee). The node S_2 receives the 41 bitcoins on behalf of client c_2 into the lightweight wallet I_2 and the crypto currency exchange S_x has been debited with 42 bitcoins. The time stamps correspond to the transaction steps as modelled in the Instruction Lifecycle Graph (Figure 2.7). The overall settlement exposure that c_2 has towards S_x is only resolved at t_{i+9}, i.e. after the transaction has been published in the next block and that block is followed by six subsequent blocks.

<u>Step 3:</u> Once c_2 has received the bitcoins and these have been confirmed, he will instruct the transfer of 41 bitcoins, 1 bitcoin transaction fee and 40 bitcoins from his lightweight wallet I_2 to reach the lightweight wallet of merchant c_1, labelled I_1.

The wallet will support the broadcasting of the transaction request and the Bitcoin network (SN) will check whether c_2 has the required amount of bitcoins to make the transaction. The instruction lifecycle will look analogous in graph theory terms to the Bitcoin transaction between S_x and c_2 visualised in Figure 2.7 above. As soon as the merchant c_1 receives the 40 bitcoins in his lightweight wallet I_1 and these have been confirmed, his settlement exposure towards c_2 as part of their trading relationship is removed (i.e. the financial leg has settled) and he can spend the bitcoins as he sees fit.

<u>Step 4:</u> Given that the merchant still wants to exchange the bitcoins into GBP, he will instruct his Cryptocurrency Exchange (located in the UK), denoted as S_y, to convert the 40 bitcoins into GBP. In this transaction c_1 is fully exposed to S_y, because the bitcoin to GBP transaction is not simultaneous as discussed above.

<u>Step 5:</u> Assuming that S_y successfully converts bitcoins to GBP, the closing transaction will be an interbank credit transfer between the bank of S_y and the bank of c_1. For this purpose S_y will again instruct a domestic payment with his bank. Settlement risk is ultimately eliminated when c_1 receives the expected GBP amount in his account as well as the accompanying credit confirmation. Note that this tends to be a legally enforceable confirmation, subject to settlement finality legislation where applicable.

2.7 BITCOIN PoW VERSUS LEGAL SETTLEMENT FINALITY

As we have seen from the above modelling exercise, functional settlement finality does occur in the PoW system of Bitcoin, subject to the proposed adjustments to the UFM model.

In order to evaluate whether Bitcoin PoW can be considered qualitatively superior to a legal approach to settlement finality (based on CPMI-ISOCO Principle 8 and associated legal frameworks) when it comes to mitigating unwinding and systemic risk, we will apply the three moments of Settlement Finality as defined by the T2S Advisory Group.

In the context of Bitcoin PoW the three moments of Settlement Finality can be interpreted as follows:

SF1: Moment of entry into the system (M_e)

In Bitcoin PoW this moment is represented by a new transaction submitted to SN that is sent by a node such as S_2 (in Figure 2.4) to the other network nodes, in order for mining and validation to begin.

Note here that the requirements of the European Settlement Finality Directive (Directive 98/26/EC) are embedded in the European system rules, determining when a transfer order has legally entered the system. In Bitcoin the system rules are represented in code rather than being defined in law.

SF2: Moment of irrevocability (M_i)

This moment in Bitcoin terms is synonymous with M_e, defined above, as transactions, once entered into the network are technically irrevocable.

SF3: Moment when the transfer is settled with finality (M_f)

The moment of final settlement in Bitcoin PoW, as expressed by the previous analysis in Section 2.6, occurs when a transaction is in a valid, mined block such that DSF = 6.

Based on these definitions we can answer research question 3 as follows.

First of all, unwinding risk cannot occur in either of the discussed Bitcoin scenarios. As explained above, once a transaction has been submitted to the first node, there is no option to unwind it because PoW is based on immutability.

For the question on systemic risk, we can examine this across two angles:

1) Assuming that the sender added a fee into the bitcoin transaction order that is sufficiently high to allow for mining of the transaction, then settlement risk is not going to arise. However, we are faced with an uncertain timeframe regarding the receipt of bitcoins by the beneficiary, given the fact that depending on the exact fee level inserted in the instruction, transactions could be de-prioritized in terms of mining. Such an outcome would represent liquidity risk on the beneficiary side as functional settlement could happen later than DSF= 6 i.e. later than the expected moment of SF3. If the delay in functional settlement is not too significant, and assuming a low transaction amount, systemic risk would not arise.

2) Assuming in a second scenario that the fee inserted is either zero or too low to trigger any miner's interest in mining the transaction, the transaction would fall into the memory pool and subsequently end up in an orphaned block, where the transaction would not be processed at all; the bitcoins would ultimately reappear in the sender's lightweight

wallet. In this instance the beneficiary would not receive any bitcoins at all, which could, in a worst-case scenario, trigger systemic risk if the expected amount were to be significant – a chain reaction could be triggered.

When considering the end-to-end transaction chain, as expressed in the 'Bitcoin Ecosystem' scenario, we recognise a second layer of transactions, the fiat currency 'on and off ramps', which behave according to the legal rules for settlement finality, if executed via compliant payment systems. Here, unwinding risk is mitigated via the use of payment systems that are subject to the legal settlement finality frameworks. Systemic risk can arise both within the Bitcoin system – as discussed above - and across the external regulated payment system space. Whilst the legal settlement finality framework ensures that in case of bankruptcy of a sender within the settlement timeframe transactions will still go through as unwinding risk is mitigated, transactions will ultimately not settle if there is no money on the day of settlement. This could lead to systemic risk and the traditional way to mitigate this risk would be by using a default fund such as is the case in the payment system EURO1 where participants effectively pay in advance for the risk of defaulting.

Under the condition that users are holding lightweight wallets with Cryptocurrency Exchanges, where the exchange effectively holds the public-private key pairs of each user, users may be subject to investment risk, analogous to customers that hold their money in accounts at commercial banks. Whereas in the latter case, a certain amount of monies held with banks is protected, e.g. in Europe under the deposit guarantee scheme, Bitcoin users have no protection at all.

Again, in case a lightweight wallet provided by an exchange is used, many of these providers offer a range of fees and associated processing times, which means that a transaction with no fee or too low a fee cannot be practically initiated in the first place. This means that liquidity risk is effectively managed from the outset, thus reducing the probability of systemic risk. In Bitcoin PoW we have the advantage that bitcoins are immediately ‘reserved’ once a transaction request is made. The ‘money’ is always there at the time of settlement, which represents a better outcome in view of supporting financial stability.

In conclusion we can say that from a practical perspective PoW can deliver superior results to the existing legal settlement finality frameworks (based on CPMI-IOSCO Principle 8 for FMIs and associated legal frameworks such as the SFD), in light of mitigating unwinding risk and systemic risk. Bitcoin PoW represents a clearer process even when compared to the alternative scenario where a default fund is used given such funds bear their own risks.

2.8 RESULTS

Having reviewed extant literature we found that settlement finality is only achieved within an existing legal framework. This restriction means that Bitcoin would not qualify for settlement finality in the legal sense.

With regard to research question 1 we find that the UFM requires a number of modifications and extensions in order to be able to capture functional settlement finality in the 'Pure Bitcoin' scenario. Having applied those enhancements to the UFM definitional framework and graphs, our modelling results show that Bitcoin does achieve functional settlement by virtue of its technological construct. In order to answer research question 1, we introduce an alternative definition of functional settlement finality that captures the notion of degrees of settlement finality (DSF) instead of a legal definition of settlement finality. This notion of degrees of settlement can be re-used for other existing and emerging DL structures.

In response to research question 2 we find that that the UFM is capable of defining functional settlement finality in the 'Bitcoin Ecosystem' scenario, subject to the modifications and expansions already discussed and applied for the purposes of modelling the 'Pure Bitcoin' scenario, with the only difference that the 'Bitcoin Ecosystem' scenario requires the application of all agent types as defined in the UFM.

In this we introduce the notion of end-to-end settlement, which reflects the fact that we have a longer and more complex chain of transactions, starting from traditional payment processes based on fiat currency and passing via the 'Pure Bitcoin' scenario, in order to eventually end up back in traditional fiat currency.

The graphs in scenario 2 reflect that the Bitcoin system at the centre has only changed in so far as we have an additional type of agent, the financial intermediary (light weight wallets, often provided by

Cryptocurrency Exchanges). These wallets can introduce fraud risks inside the system in case of inadequate security levels, but there is no particular increase in settlement risk compared to scenario 1. However, we do observe additional settlement risk arising from elements that are not strictly part of the internal Bitcoin system, i.e. outside the 'Pure Bitcoin' scenario. A particular focus here is on the process of currency conversion performed by Cryptocurrency Exchanges, which are still relatively new providers and in many instances still unregulated. As these concentrate risk, similar to FMIs, they would need to be regulated in a similar way, i.e. in case of future systemic importance they should be required to ensure PvP processes such as those taking place in the context of CLS. Repeated cases of Cryptocurrency Exchanges not properly settling conversion transactions and in several cases stealing bitcoins from their users are evidence of unmanaged risks. These types of risks should be countered by appropriate conduct of business and consumer protection regulation. Given that in the extended 'Bitcoin Ecosystem' process bitcoins have to be converted from and into the 'old world' of fiat currencies, this requires the combination of internal settlement, based on our new DSF definition, and external settlement according to the traditional definition of settlement finality, i.e. the legal framework.

And finally, by comparing and contrasting Bitcoin PoW with the legal notion of settlement finality under research question 3, we can state that functional settlement finality in Bitcoin is preferred (even when compared to the default fund model) to legal enforceability under the (severe) condition that the issues around energy consumption, speed, scalability, the 51% attack risk and the fork related risk of users not receiving the newly created coins (as shown e.g. in the case of the fork with Bitcoin and Bitcoin Cash) are mitigated. This means that the Bitcoin blockchain is at present not practically suitable for the trusted environment of the regulated financial industry.

2.9 DISCUSSION

Our study provides insights into the potential of technology innovation for systemic risk management in the context of payments. We demonstrate that, subject to a number of modifications and expansions of the UFM we can model the Bitcoin system and find that functional settlement finality is achieved through a distributed and immutable process based on the PoW blockchain.

2.9.1 Implications for theory

Our exercise identifies gaps in literature as these relate to settlement finality in distributed systems that have no applicable regulatory frameworks and provides for a new definition of functional rather than legal settlement finality that can apply to the Bitcoin PoW blockchain.

2.9.2 Practical implications for the industry and regulators

Whereas immutability of the blockchain is akin to the literature requirement of unconditionality, distribution of the settlement process is something completely new. This finding is of particular interest as achieving functional settlement finality in the absence of intermediaries such as FMIs, which normally play the settlement entity role, allows us to imagine a financial market without FMIs. Whilst FMI driven settlement has a legal basis, because transactions can be (technically) reversed – i.e. participants need the ability to have legal recourse – the Bitcoin process provides technical irreversibility of transactions, in which case it could be argued that participants do not require the ability of legal recourse.

The broader set of FX risks, counterparty risks, investment risks as well as outright fraud risks that arise from new services and providers that bridge bitcoins and fiat currencies in the context of the broader 'Bitcoin Ecosystem' scenario requires regulatory attention.

2.9.3 Limitations and future research suggestions

The main limitation of our research relates to the fact that we only examine blockchains based on the PoW consensus algorithm, exemplified by Bitcoin, which has very specific features and implication for settlement finality. Because Bitcoin has been designed to achieve consensus in a fully decentralized and trustless environment of participants, it is not the optimal solution for the regulated financial industry, which by virtue of regulation creates a certain level of trust and identification of participants. First of all transaction processing is slow, compared to existing solutions in financial services, such as for example credit card transactions. At the time of writing the Bitcoin system achieves 4 to 7 transactions per second, compared to Visa, which at peak times processes more than 2000 transactions per second.[13] Increasing the transaction capacity in order to be able to compete with mainstream retail payments would open up vulnerabilities, which would require an overhaul of the consensus mechanism. Secondly, PoW is inefficient and costly from an energy perspective as the cryptographic calculations required to win the mining contest (which prevents double-spending) consumes a lot of computing power and thus energy, including for cooling the computers. One Bitcoin transaction in 2018 consumed 1005 kilowatt hours of energy, compared to 100,000 Visa transactions that consumed 169 kilowatt hours of energy (see www.statista.com). A third issue, however less problematic in Bitcoin given the large amount of nodes and the economic incentives of mining as discussed, is that there is still a possibility of double spending in case of a 51% attack.

[13] For further details see: https://www.visaeurope.com/enabling-payments/processing (last accessed 15/04/2019)

More practical research and experimentation is therefore required in order to design DLs that can combine the benefits of Bitcoin in relation to managing unwinding and systemic risk and at the same time cater for speed, scale and security in line with the needs of the regulated financial industry. Whereas PoW is arguably one of the most mature and effective solutions for consensus in an open trustless environment, the landscape of other consensus algorithms is rapidly evolving. Many of the emerging industry-led solutions tend to be based on permissioned DLs (i.e. only open for a select group of identified participants), achieving high throughputs, scalability and low cost, which however balances with being semi-trusted and often more centralised (e.g. Hyperledger, Stellar, Ripple). Another consensus algorithm is the so-called 'Directed Acyclic Graphs' (DAGs), which is a form of consensus that does not even use the blockchain data structure and instead handles transactions mostly asynchronously. In this category we also find the Serialization of 'Proof-of-work Events: Confirming Transactions via Recursive Elections' (SPECTRE), hailed by some experts as the potential way to fix Bitcoin as it can reach scalable consensus, where rather than 'the longest chain wins' those 'blocks with the most children win'. A very recent consensus algorithm (still in patent process)[14] is the Distributed Random Master Election (DRME), a method for a leader election amongst autonomous processes without client involvement. DRME is based on an efficient distributed random number generation algorithm and its semi-interactive protocol ensures byzantine fault tolerance and supports the dynamic joining and leaving of processes. This method minimises the risk of an attacker controlling the leader election and is the first of its kind that uses techniques that solely build on a random number to elect a leader, whereas randomness so far is only used to create groups or subgroups of nodes within a network. The combination of speed

[14] The DRME patent has been filed in January 2019 under Registration Number 19 450 001 3 for a European Patent with the Austrian Patent Office.

(election done in only one round), efficiency (no difficult mathematical computation needed) and attack-resilience (due to complete randomisation) are promising indicators that this could be a solution for the regulated industry. These are early days and potential vulnerabilities and attack vectors of some of these emerging algorithms have not been sufficiently tested.

In addition, the industry's desire to change the underlying protocol in case something does not work according to expectations is another area, which would require a very different design approach compared to the way Bitcoin operates. Governance and different degrees and qualities of distribution in DLs for the regulated industry will thus become an important future priority in addition to standardisation.

A key question here is whether we would end up in a paradoxical situation if we apply regulation to a trustless distributed system by turning it into a centralised system as a consequence. The assumption that centralisation equates to trust is in our view no longer relevant, even if the centre is regulated. In fact, this statement is reflected in one of the key motivations of Bitcoin itself, which was to create an alternative to the regulated industry, where central authority was seen as unjust, power-hungry, displaying flawed and even criminal behaviour. Efficiency, speed, and low cost are important elements that a DL and its underlying consensus should achieve, but what is also required is to mitigate dishonest behaviour – i.e. factor in the risk of double-spend and develop effective incentive structures to counter this risk, even if the participants in a DL are 'trusted', identified and regulated participants – as well as to allow for technical distribution of processing and privacy in areas where it makes sense.

Chapter 3

The Future of Correspondent Banking Cross Border Payments

Disclaimer: This Chapter forms the basis of a paper co-authored with Prof. Barbara Casu. A SWIFT Institute Grant supported this research and the paper has been published in Q4 2018 as a SWIFT Institute Working Paper (see: https://swiftinstitute.org/research/the-future-of-correspondent-banking/)

3.1 INTRODUCTION

The ability to transfer money across borders in a safe and secure way is an indispensable requirement for the global economy. Until now the main method of executing money transfers globally is via correspondent banking arrangements. Correspondent banking covers the three pillars of cross-border payments, foreign exchange (FX) transactions and trade services. More than 11,000 financial institutions (FIs) engage with each other across more than 1 million bilateral correspondent banking relationships (CPMI, 2016).

At the global aggregate level, cross-border payments reached 22 billion in volume, translating into 22075 billion $ of value based on figures from 2016 (Boston Consulting Group, 2018). According to McKinsey (2016), despite the fact that cross-border payments represent only 20 percent of total payment volumes, "*they comprise about 40 percent of global payments transaction revenues (i.e., transaction related fees and float income), and generated $300 billion in global revenues in 2015*", a sizeable business.

In recent years, new technologies and infrastructures have been developing, presenting both opportunities and challenges for the banking industry. For example, several new types of cross-border payment solutions have emerged both in the retail and wholesale payments space. In retail, we have seen the rise of non-bank payment intermediaries, which leverage various technologies and network types (including mobile networks, e.g. M-Pesa in Kenya) and the emergence of schemes such as the Asian WeChat Pay (owned by Tencent) and AliPay (owned by Ant Financial, an affiliate of Alibaba), in addition to other established players such as Transferwise and Paypal. However, cross-border payment intermediaries often rely on correspondent banking structures to provide FX and settlement services. Furthermore, regional initiatives exist or are being explored for both Automated Clearing Houses (ACH) and Real Time Gross Settlement (RTGS) system linkages. SEPA is a good example of an initiative to simplify cross-border retail payments across a single currency area and beyond (Wandhöfer, 2010).

In addition, we have seen the emergence of cryptocurrencies such as Bitcoin (and 1000+ other types of altcoins). These solutions are offering a banking-free way to transfer value across borders and have found some appeal in the context of non-government controlled transactions as well as with regard to financial inclusion objectives across emerging economies. Focussing on the underlying Distributed Ledger Technology (DLT) we also begin to see experiments that look to reengineer fiat currency based cross-border payments.

With the emergence and maturing of new technologies, including cryptography, cloud computing, the Internet of Things (IoT), as well as techniques such as homomorphic encryption and the prospect of Quantum computing developing rapidly, there is a need to evaluate how far and in what manner a future global banking system can leverage these new digital pillars. At the same time the industry needs to address key questions, such as how to support business activities resulting from these new technologies and the business models that emerge, many of which require seamless integration of payments into service models (e.g. Uber). Whilst some of these emerging technologies will play a key role in the future, it is essential to align the deployment of those with clear regulatory, compliance and governance models as well as legal rules to ensure a practically workable and legally enforceable system that can be effectively – and efficiently - supervised. Other questions around technological maturity, scalability and interoperability between DLT and existing systems as well as between DLT implementations will also need to be addressed.

The overarching rationale to strengthen cross-border payments, and in particular the settlement of payments, is reflected in their importance for financial stability. Despite the enhanced capital and liquidity requirements, including intraday liquidity requirements, as well as leverage limits imposed on FIs by the Basel framework (Basel III), the potential risks to financial stability lie with the actual assets that FIs hold. As the quantitative easing (QE) strategies initiated by major central banks in the aftermath of the global financial crisis are now slowly coming to a halt, liquidity becomes only available through pledging government bonds to central banks. If those bonds become 'junk' – such as during the Greek crisis - then the cash they can generate is minimal, which could lead to another Lehman Brothers scenario for many FIs. This is why the ability to settle even during stress events will become more important going forward.

Against this background, this Chapter seeks to develop the building blocks for a future blue print for cross-border payments. A particular focus will be placed on the wholesale aspects of these flows, as they constitute a systemically important area of business with FI and corporate transactions representing 80% of the cross-border transaction value and 20% of the overall transaction volumes.

A first step in our analysis consists of the identification of the current challenges of the existing correspondent banking model. We then propose ways in which the industry can leverage new technologies and processes, complemented by standards, governance and policy recommendations in order to be able to deliver a substantial improvement in cross-border wholesale payments.

The remainder of this Chapter is organised as follows. Section 3.2 provides an overview of the current way in which cross-border wholesale correspondent banking payments operate. It develops the context of regulatory and market challenges of this business and explains how the correspondent banking market is organised. Section 3.3 presents a review of the literature on key developments in the payment space. Section 3.4 sets out the research questions of this Chapter and describes the research methodology. Section 3.5 provides a summary of the empirical findings, covering the identified pain points and shortcomings in cross-border correspondent banking payments resulting from an on-line survey. Section 3.6 sets out the key requirements for the future of cross-border correspondent banking payments. Section 3.7 develops a set of design scenarios for an improved global cross-border payment process, based on the outcome of focus group meetings with key stakeholders (banks, central banks, regulators, technology providers). Section 3.8 combines an evaluation of the discussed scenarios with a set of policy and standards recommendations that will enable or support the delivery of improvements in the cross-border payments market. Section 3.9 concludes.

3.2 CORRESPONDENT BANKING: CROSS-BORDER PAYMENTS

In order to develop a set of design and policy proposals with a view to improving the state of correspondent banking cross-border payments, we will need to first of all understand what correspondent banking payments are and how they operate.

3.2.1 Definition of correspondent banking

There are various definitions of correspondent banking in the market today. In general terms, correspondent banking can be defined as *"an arrangement under which one bank (correspondent) holds deposits owned by other banks (respondents) and provides payment and other services to those respondent banks"* (BIS, 2016). Further expanding on this concept, we particularly like the definition that was developed by the Wolfsberg Group, which states that *"[c]orrespondent banking is the provision of a current or other liability account, and related services, to another financial institution, including affiliates, used for the execution of third-party payments and trade finance, as well as its own cash clearing, liquidity management and short-term borrowing or investment needs in a particular currency."* (The Wolfsberg Group, 2014).[15]

Essentially the correspondent banking model operates via an international network of FIs, which have bilateral account relationships with each other. A bank that is obtaining correspondent banking services from another bank holds a so-called *Nostro* (Latin: ours) account with such provider bank, where the account is denominated in a foreign

[15] The Wolfsberg Group is an association of 13 global banks which aims to develop frameworks and guidance for the management of financial crime risks

currency. From the provider bank's side this same account is called *Vostro* (Latin: yours) account. This tightly woven network of FIs, in which trust plays a central role, has developed to global dimensions over the last centuries. Despite the distributed nature of correspondent banking, systemic risk can be significant as we have seen during the banking crisis, which is why improving financial stability in this space is of crucial importance.

3.2.2 Key risks and challenges in correspondent banking

Key risks of the correspondent banking cross-border payments business include: market, FX, credit and counterparty and regulatory risk (e.g. AML and CTF). Furthermore, technology and operational risks, as well as risks regarding the availability and cost of liquidity to support the business, do arise. In addition, correspondent banking cross-border payments are relevant for financial stability.

In today's cross-border high value interbank payment space, FIs often lack real time visibility of the settlement status of transactions as these payments move along the correspondent banking *Nostro*/*Vostro* account chain. High value transactions that are not properly settled could create a chain reaction in case of default of one of the parties. Furthermore, the opportunity cost of wrongly assessed and misplaced intraday liquidity, as well as costs associated to missed payment deadlines, creates further challenges in cross-border payments. The risk around correspondent banks' intraday credit lines (usually uncommitted) versus truly funded positions is an area that will remain a risk management priority for clearing banks as long as there is no visibility on if and how a payment is funded.

An important challenge for the industry, as well as for regulators, is the continued decrease in correspondent banking relationships which results in lengthening payment chains and increasing reliance on fewer correspondent banks (FSB, 2017). In addition, it may affect a country's or jurisdiction's ability to send and receive international payments. This, in turn could drive some payment flows into the unregulated sector, with potential negative consequences for international trade, growth, financial inclusion and financial stability.

This 'de-risking' process has many causes, but regulatory compliance is certainly playing a role. Because of increasingly tightening regulatory requirements (AML and CTF as well as regulatory sanctions requirements that bring with them the risk of regulatory fines) by key jurisdictions, such as the US and Europe, seventy-five per cent of global bank providers in this space have reduced their correspondent banking relationships (IMF, 2017) or withdrew from this business altogether. As a consequence, the market has seen an growing concentration trend, where almost half of the banks that took part in the Financial Stability Board (FSB) survey in 2017 reported reliance on no more than two correspondents for the majority of their cross-border wire payments traffic (FSB, 2017). We will be developing a set of policy recommendations in Section 8 to address these challenges.

3.2.3 The cross-border payments process flow

Despite the aforementioned risks and challenges, cross-border correspondent banking payments is a business characterised by ubiquity and its ability to provide reach, a core advantage over current alternative solutions. At the heart of the correspondent banking payments process we have the two key pillars of messaging and settlement.

For messaging in cross-border payments, the most widely used solution is provided by SWIFT, which enables payment messaging via its secure interbank network.[16] The payment message then normally flows through an entry posting system, which creates a debit to the sender's account in their books and either a credit to the beneficiary's account if this is held with the same correspondent or a posting to the payment system queue for settlement over the RTGS or other payment system, depending on value. Once the original payment instruction message is received by the correspondent bank, an acknowledgement of receipt is sent back to the sending bank.

Settlement can be defined as "*the discharge of an obligation in accordance with the terms of the underlying contract*" (BIS, Glossary), which can happen in commercial bank or central bank money. The main method for settlement in the correspondent banking space is commercial bank credit settlement via the *Nostro*/*Vostro* accounts across the payment chain. The final payment, however, may be settled in either commercial or central bank money, e.g. in case the last payment leg is processed by a local Payment Market Infrastructure (PMI), such as an ACH or RTGS system.

For international settlement in central bank money there is a global central counterparty that supports centralised settlement finality for cross-border FX transactions, the CLS (Continuous Linked Settlement) Bank - a global FMI. CLS was established to mitigate the risk of counterparty failure in the FX market under the auspices of major central banks and it enables the netting and settlement of FX transactions between participant members, and indirectly on behalf of end users, including FIs.[17]

[16] National payment systems do not generally use SWIFT and can operate on a variety of messaging systems. Even for cross-border payments there are alternatives to SWIFT.

[17] Although CLS is undoubtedly the most important global counterparty for cross-border FX transactions, it must be noted that they only cover a subset of the world's currencies (18 of the most actively traded currencies globally).

CLS significantly reduces the gross intraday liquidity required to settle individual FX transactions for an active FX bank on a daily basis but it does introduce a time specific intraday liquidity position, the pay-in/pay-out time for each currency – which in many instances is outside of 'normal' settlement times. CLS of course is primarily concerned with FX settlement and addresses the well-known Herstatt Risk but does nothing for the greater value of securities payment legs or clean payment settlements (i.e. not involving FX).[18] Today, according to CLS, around 40% of cross-border FX transactions are processed via CLS.

From a process perspective, correspondent banking cross-border payment transactions can include multiple banks and can be executed via two different methods: the 'serial method' and the 'direct plus cover' method.[19]

1) The 'serial method', a step by step process of payment instructions, e.g. a supply chain payment from Tokyo to Mexico, using SWIFT MT103 messages, where the USD will be cleared and settled via an FMI in the US (where the US FMI uses an MT103 equivalent message type) and then credited to the beneficiary Bank D in Mexico, by its USD correspondents Bank C (see Figure 1).

---

[18] "Herstatt risk" is an alternative term for settlement risk, with particular reference to FX transactions. The name comes from the collapse the German bank Herstatt in the 1970s.

[19] Here we refer to transactions that are executed via the SWIFT network.

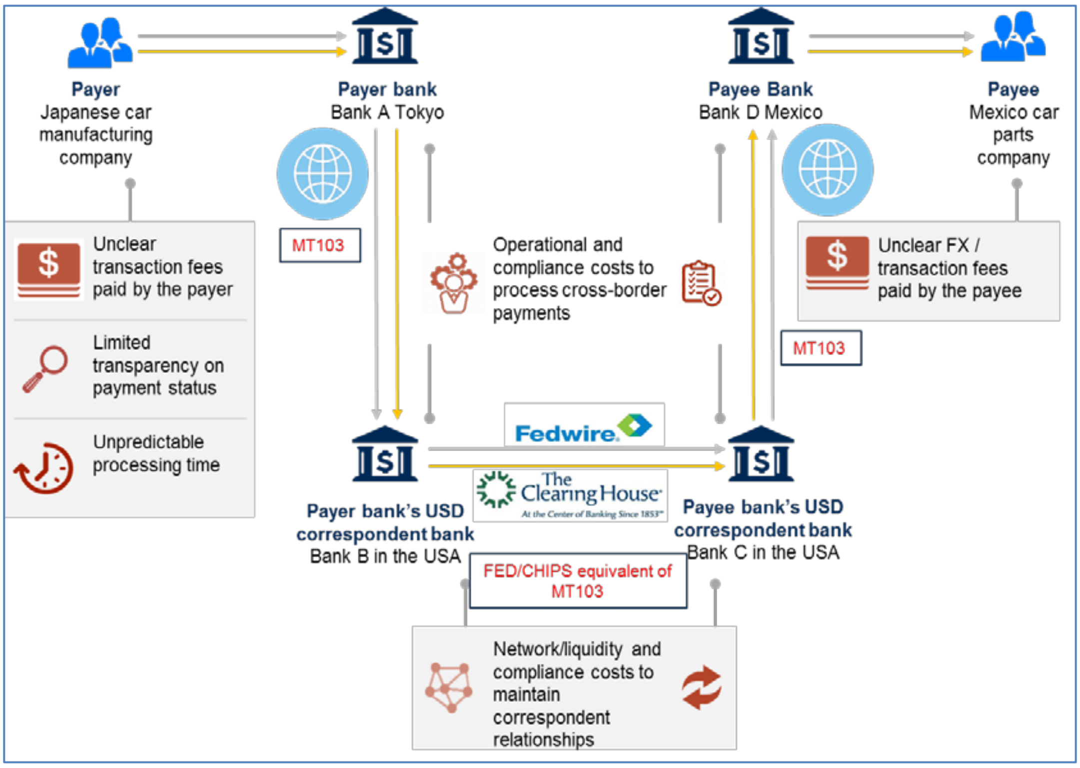


Figure 3.1: Correspondent Banking Payments Process "USD Serial Payment from a Payer in Japan to a Payee in Mexico" (*source : R. Wandhöfer*)

2) The 'direct plus cover' method is at work where the client payment instruction will go directly from the USD correspondent bank B[20] to Bank D in Mexico (using a SWIFT MT103 message), whilst the settlement of USD will again take place between the two USD correspondent banks via the FMI. A SWIFT MT202COV message is used between the USD correspondent Bank C and Bank D, whereas an MT202COV equivalent message is used for settlement across the US FMI. In this second scenario the payment instruction and the settlement of funds therefore travel separately (see Figure 3.2).

[20] Note that bank A could also potentially send the payment as a direct MT103 message to bank D but many banks leverage their correspondents for this as large Global Transaction Banks have a broader RMA (Relationship Management Agreement) networks and bilateral RMAs are necessary between banks to communicate directly via SWIFT.

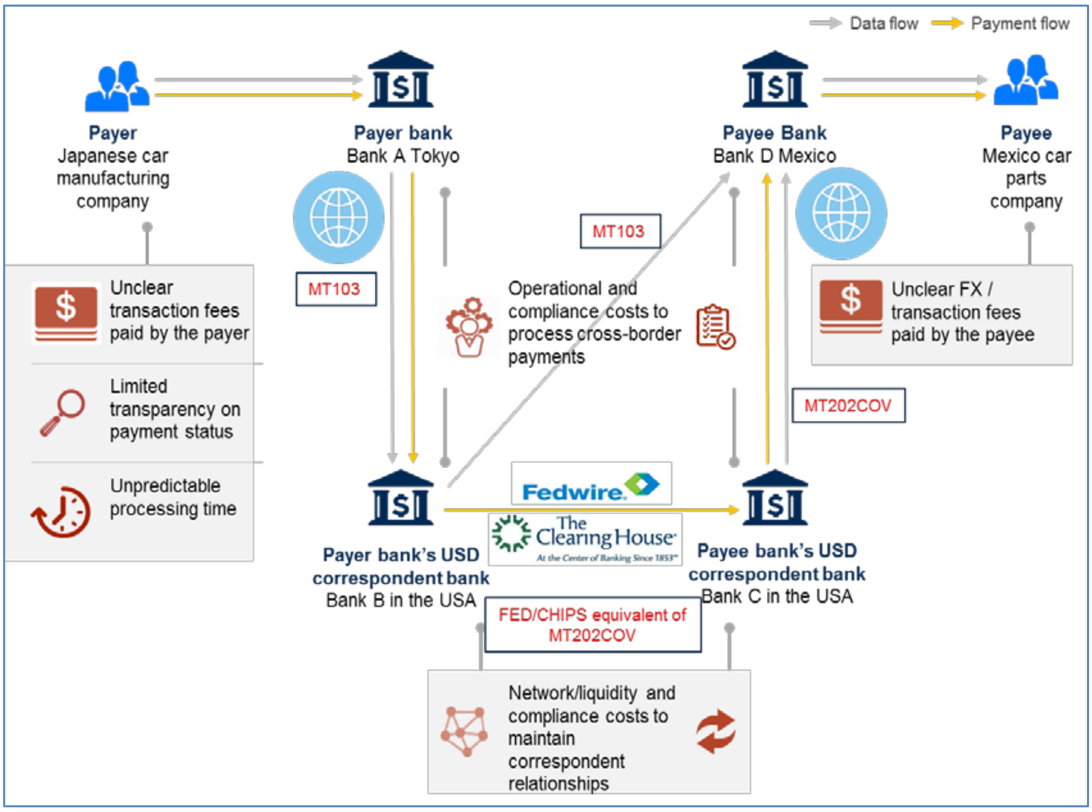


Figure 3.2: Correspondent Banking Payments Process "USD Direct and Payment from a Payer in Japan to a Payee in Mexico" (source : R. Wandhöfer)

To avoid the transparency issues that were associated with the use of the MT 202 format for cover payments, where the clearing banks were generally not aware of the actual payment instruction and only 'blindly' operated the settlement of the financial flow and associated FX (see BCBS, 2009 and CPMI, 2016), the MT202COV message was introduced in 2009, so that the underlying settlement could be sanction screened, similar to the original MT103 message. Counterparty risk may arise as banks can chose to credit the next bank in the chain before having received the cover payment.

There has been historically a lack of transparency related to the status of payments.

There are many factors that can influence the speed of a payment, for example Spot FX in case banks do not have the liquidity in the correct currency or the fact that an RTGS system is closed when sending the payment. Depending on the parties and systems involved, several SWIFT messages could be used in the process. In addition, some national payment systems (e.g. Fedwire and CHIPS in the US, Australian, Swiss and Japanese RTGS systems) do not use SWIFT messages.

In terms of costs of cross-border payments, transaction fees can be charged by each bank in the chain. Various charging models based on different charge codes exist (e.g. OUR/BEN/SHA)[21] and charging can depend on the market that the payment is being sent to and whether for example credit fee deduct practices are widely used or not. In addition, messaging fees for network usage, such as those for using the SWIFT network, do apply. KYC/AML/CTF checks are conducted by each bank and manual intervention is often necessary in case the payment stops. Given the fact that multiple banks are involved in the payment chain, multiple break points can arise, thus resulting in payment delays.

In addition, network and liquidity costs are involved in maintaining correspondent relationships. Costs arise for each bank that is involved in the process of funding interbank accounts and managing exposures. The majority of frictions and inefficiencies tends to emerge in the context of local market regulatory requirements, time zone issues and restricted FX in certain markets. Whereas a large portion of payments are processed straight through (STP processing), the remainder tends to increase costs due to various types of exceptions such as a sanction hit, returns or missing information. From a financial stability perspective, the fact that banks often operate on the basis of

[21] Charge code OUR means that the payer bears all the transaction charges; charge code BEN refers to the payee paying all the transaction charges and charge code SHA represents the sharing of the transaction charges between sender and receiver of the payment.

uncommitted intraday credit lines creates another level of complexity and risk, which led to significant problems during the financial crisis.

To summarise, despite the importance of correspondent banking relationships to facilitate global trade and economic activity, the current model presents a number of challenges. In the next section, we aim to identify and validate these pain points.

3.3 LITERATURE REVIEW

There has been a growing literature on correspondent banking over the last decade. Primarily as a consequence of regulatory fines applied in the AML and CTF context, governments and market participants had to deal with the increasing challenge of correspondent banking providers withdrawing services from banks and PSPs that they deemed to be too risky. However, while there are a number of supranational organisations and central banks that have developed analysis and policy papers addressing the topic (see for example Alleyne et al. (2017), FSB (2017) and various consultancy reports), little attention has been paid so far by the academic literature, both theoretical and empirical.

On the other hand, there is a growing interest and emerging research literature on financial technology (or FinTech) and on crypto-currencies and crypto-assets. The way in which new technology is transforming access to finance for individuals, start-ups, Small and Medium Enterprises (SMEs) or corporates (for example through online platforms for crowd-funding, marketplace/peer-to-peer lending, and third-party payment providers) is also gaining attention. There are a number of descriptive works covering these emerging issues, particularly in the form of consultancy reports or books (see, for example PwC (2017) Global Fintech Report).

For the purpose of this analysis, we will focus our literature review on three related areas: correspondent banking; settlement risk and finality; and new technologies in payments.

3.2.1 Correspondent banking

The decline in the number of correspondent banking relationships is a source of concern for the international community, as evidenced by the attention paid to the issue by supra-national organisations, such as the FSB, the BIS, the IMF and the World Bank, as well as leading central banks. Regulators worry that, in affected regions, the decline of correspondent banking may impact the ability of firms and households to send and receive international payments. This may drive some payment flows outside the regulated banking system, with potential adverse consequences for the stability and integrity of the financial system (FSB, 2017). In particular, the risks associated to money laundering and terrorist financing form a key part of the risk of flows passing through informal systems. Another risk is that those banks that have been 'de-risked' could become 'nested' correspondents, i.e. they would maintain correspondent accounts through those banks that have managed to maintain their correspondent relationships. This would translate into longer interbank chains and the risks of separation of related inter-bank payment messages.

To find out whether such a range of 'de-risking' is indeed happening, the World Bank (2015), with support from FSB and the CPMI, surveyed banking authorities and banks worldwide to examine the extent of withdrawal from correspondent banking, its drivers, and its implications for financial exclusion/inclusion. The participants in this survey, carried out in 2015, included 110 banking authorities, 20 large banks, and 170 smaller local and regional banks. The World Bank survey confirmed that most of the participants were experiencing a decline in correspondent banking relationships, particularly international banks. In terms of products and services, the most affected by the withdrawal of correspondent banking are: international wire transfer; clearing and settlement; check clearing; trade finance; cash management services; investment services and, to a smaller degree, foreign exchange services and lending. In addition, the ability to conduct foreign currency denominated capital or current account transactions in US dollars, Euro, pound sterling, and Canadian dollar in particular has also has been significantly affected. Most respondents indicated the following as the main reasons driving their decisions to end correspondent banking relationships: economic slowdown in some regions and regulatory risk (AML/CTF), including concerns about international and national sanctions. Overall, the results of the survey indicate that, while large banks might be cleaning up their balance sheets and ending relationships with customers deemed to be risky, these risks might end up in sectors that are less transparent and less regulated, thereby increasing overall systemic risk. This is a cause for concern for regulators. To address these concerns Grolleman and Jutrsa (2017) present a framework to monitor the development of correspondent banking relationships, to be used by national central banks and supervisory authorities, based on the fact that national authorities can access more granular, bank level data, and are better placed to conduct detailed market analyses. The monitoring framework proposed by Grolleman and Jutrsa (2017) includes two scenarios: (1) a Minimum Scope Template for collecting data from banks and the conduct of a full assessment of the domestic banking system's ability to access the international payment system, and (2) an Expanded Scope Framework, which includes the values and volumes of individual transactions using respondent banks' SWIFT payment data.

In March 2018, the FSB published a progress report addressing the decline in correspondent banking, following its four-point action plan of November 2015 (examining dimensions and implications of the issue; clarifying regulatory expectations; building domestic capacity and strengthening tools for due diligence in correspondent banking). The progress report highlights promising developments. These include the Wolfsberg Group updating its correspondent banking due diligence questionnaire, which will support a more standardised collection of information on respondent banks. It is important to note however, that whilst increasing the efficiency by streamlining the due diligence process, the practical problem in the market is that there are banks seeking correspondent services that do not have the necessary controls in place. The FSB also reports on the latest additional steps including: (i) data collection and analysis: the update of global data on correspondent banking relationships, using data provided by SWIFT as of end-June 2017; (ii) clarifying regulatory expectations through new guidance by the Financial Action Task Force (FATF) and revised guidance by the Basel Committee on Banking Standards (BCBS); (iii) further steps to promote the coordination of domestic capacity building to improve and build trust in the supervisory and compliance frameworks of affected jurisdictions; (iv) develop technical solutions aimed at improving the efficiency of due diligence procedures and reducing compliance costs; and (v) stocktake on remittance service providers' access to banking services, including recommendations to improve accessibility.

3.2.2 Settlement risk and finality

Settlement risk is the risk that settlement in a funds or securities transfer system will not take place as expected and may comprise credit and liquidity risk, as well as operational and legal risk, where all of these have the potential to trigger systemic risk (ECB, 2010). Secure settlement of payments is therefore at the heart of protecting the stability of the financial system. It is in this context that the role of payments has gained such importance over the last decades.

In order to remove settlement risk, settlement needs to be final. Final settlement is defined as "*the irrevocable and unconditional transfer of an asset or financial instrument, or the discharge of an obligation by the FMI* [financial market infrastructure] *or its participants in accordance with the terms of the underlying contract. Final settlement is a legally defined moment.*" (BIS Glossary, 2018).

Settlement finality can occur in different qualities of settlement assets, reflecting different levels of risk. For example, settlement in central bank money is considered the safest settlement asset (BIS, 2003) but can only occur in a central bank RTGS system and between direct participant accounts in the books of the central bank. Unless an FI holds an account at the central bank, all other 'final' settlement is in commercial bank credit, represented by commercial bank account balances (King, 2016). To note here is that FIs settling in central bank money can also be leveraging intraday liquidity lines for this purpose.

Settlement in commercial bank credit, where this money represents a liability of a commercial bank, "…*carries a risk: settlement funds may not be available in the event of the insolvency of the commercial bank that is providing the settlement services.*" (Francioni and Schwartz, 2017). This represents a key risk in correspondent banking payments.

In parallel to the work of central bankers and policymakers, there has also been an increased academic interest in payment economics, a strand of literature which examines the purpose of the payment infrastructure and its design in terms of mitigating settlement risk that can arise between counterparties as well as in view of providing efficiencies and the ability of economic actors to transact. Wandhöfer and Berndsen (forthcoming) provide a comprehensive review of the literature on payment finality and settlement (see Chapter 2).

3.2.3 Innovation in payments

Beyond these developments, the payment services sector has seen considerable technological change and has been subject to increased regulatory scrutiny and reforms. Examples of significant innovation in the retail payment space include the SEPA initiative in Europe (Wandhöfer, 2010) and the arrival of real-time retail payment systems.

At the same time, the wholesale payment space has moved from deferred net settlement systems (DNS) to RTGS systems and several central banks are currently in the process of renewing their systems (e.g. Bank of England RTGS review). The payments sector has also seen the emergence of a range of new providers, such as Google, Amazon, Apple and PayPal, offering various digital wallet or e-wallet products, specific methods for payments over the Internet and mobile payment services and applications.

There is now a rather sizable volume of research on FinTech, largely produced by consultancy companies, incumbent firms, industry associations and regulators, although academic studies are also emerging. The past decade has seen an increasing number of FinTech start-ups and non-bank PSPs entering the payment arena, taking advantage of regulatory change (such as the European Payment Services Directive 1 and 2) and new technologies, including cloud-based solutions and application programming interfaces (APIs).

Most economists agree that the future of money will be digital. Bofinger (2018) identifies four major areas where digitalisation could modify the traditional forms of money and credit and as a consequence modify the theory and practice of monetary policy:

- the substitution of cash with electronic money (in a retail payments context);
- the substitution of traditional bank deposits and bank notes with cryptocurrencies;
- the substitution of bank deposits with central bank deposits for everyone ('universal reserves');
- the substitution of bank lending with peer-to-peer lending on the basis of digital platforms.

Banks face new challenges, and their central role in the payment system could be diminished. The impact of new technologies in payments, particularly digital and crypto currencies, is still unclear. The potential of DLT for wholesale payments is increasingly interesting and a number of players believe that DLT can be leveraged to transform the payment industry, including correspondent banking.

Against this background, the question of what the future of cross-border payments will look like is becoming more and more relevant and will be explored throughout the remainder of this Chapter.

3.4. RESEARCH QUESTIONS AND RESEARCH METHODS

With the arrival of new technologies such as DLT and digital or crypto currencies, the question is whether we may be able to create an architecture and process that would finally deliver the long-term objective of a global payment system and currency? Our research provides a step forward on this quest by posing the following questions:

1) What are the correspondent banking industry's major pain points with the current way the market operates?

2) What key requirements would an improved future cross-border payments model need to satisfy?

3) What could a viable design for future cross-border payments look like?

4) Which standards, regulatory and governance related principles should be applied in order to support such a future model?

Our research strategy includes a combination of theoretical and empirical work. To address the first question, we have designed and carried out an on-line questionnaire aimed at industry participants. For the other three questions we have held industry focus group meetings.

3.5 EMPIRICAL FINDINGS: SHORTCOMINGS IN CROSS-BORDER PAYMENTS

3.5.1 On-line questionnaire

We begin with a review of the existing technologies and try to assess the key frictions as perceived by market participants. To this end, a short online survey (see Annex 3.1) designed to identify the key pain points and issues faced by banks in the cross-border payment space was sent to more than 2,000 bank contacts during the months of September and October 2017. We targeted industry participants across the banking, FI and non-bank payment service providers, as well as the industry expert universe.

The questionnaire had two main aims:

- Validation of pain points
- Innovation approach

Although the number of respondents was lower than we anticipated (with a response rate of around 5%) we had nonetheless 95 respondents, from 37 countries. The level of responses was unfortunately not sufficient to carry out statistical analysis of the results.

Most respondents' organisations were headquartered in Europe (over 50%), with organisations from the Asia-Pacific region ranking second, followed by the U.S.A. Most respondents work for banking institutions (around 90%). We had an almost even split between Providers (45%) and Users (55%) of correspondent banking services, as illustrated in Figure 3.3 below. Although the questionnaire allowed for respondents to indicate their job description, very few decided to do so. In our context, this is not a major shortcoming as we were more interested in the responses. In addition, as we targeted SWIFT users and clients, we can assume that respondents had a good knowledge of the field.

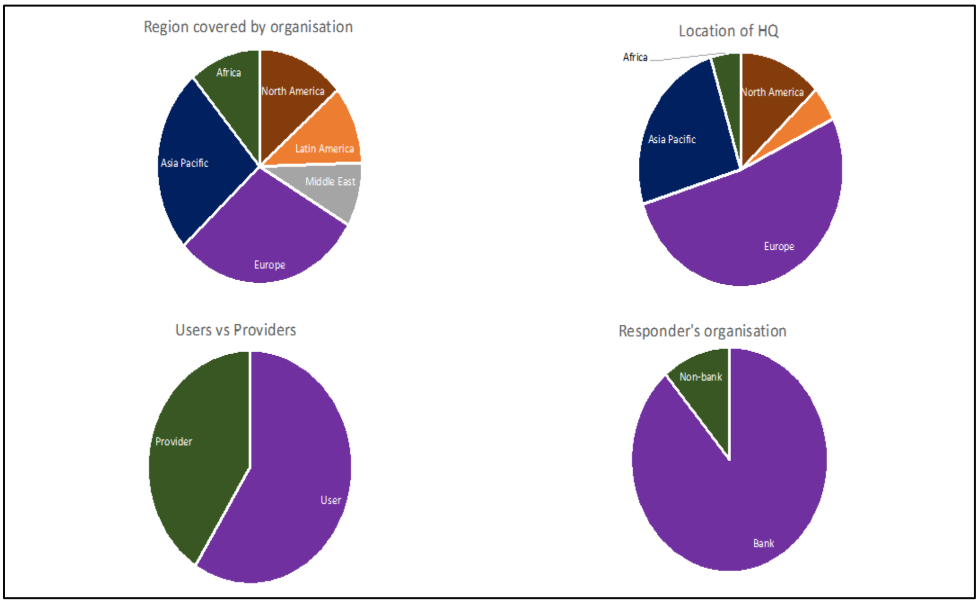


Figure 3.3: Characteristics of respondents

Tables 3.1 to 3.3 below illustrate the answers to the on-line questionnaire. Table 3.1 reports all respondents; Table 3.2 illustrates possible divergences of views between Users and Providers while Table 3.3 illustrates views and perceptions in different regions (Europe, Asia & Africa and the Americas).

Table 3.1: Percentage of respondents that strongly disagree, disagree, are undecided, agree or strongly agree with statements describing costs, information provision and technology development (all)

Statement	Strongly disagree	Disagree	Undecided	Agree	Strongly agree
1A	2	14	34	28	19
1B	0	12	28	42	16
1C	3	9	23	45	18
1D	0	5	34	42	16
1E	0	12	13	45	27
2A	0	6	8	42	42
2B	0	6	8	49	34
2C	0	0	7	43	48
3A	5	7	33	38	15

1A) Direct costs for Messaging Fees charged by the network are too high. **1B)** Fees charged by my bank provider are too high. **1C)** Liquidity related costs for this business are too high. **1D)** Capital related costs for this business are too high. **1E)** Costs related to counterparty and liquidity limits, fails in STP and incorrect processing are too high. **2A)** There is a lack of information throughout the lifecycle of the payment. **2B)** There is a lack of enhanced data and incomplete transaction reference data creates problems to reconcile transactions. **2C)** There is a lack of visibility of transaction related costs, i.e. who has paid which fees to whom for validation of AML/CTF, counterparty risk, liquidity reporting and credit limit. **3A)** Do you believe that Blockchain/Distributed Ledger Technology could be deployed as the basis for a new generation cross-border payment network?

Table 3.2: Percentage of respondents that strongly disagree, disagree, are undecided, agree or strongly agree with statements describing costs, information provision and technology development (Users v Providers)

Statement	Users			Providers		
	Disagree	*Undecided*	*Agree*	*Disagree*	*Undecided*	*Agree*
1A	21	31	47	11	41	47
1B	11	24	63	17	38	44
1C	6	27	65	23	14	61
1D	3	34	62	11	26	61
1E	6	9	83	23	17	58
2A	6	9	83	2	5	91
2B	6	8	85	8	8	82
2C	1	8	90	2	8	88
3A	9	36	54	23	32	44

1A) Direct costs for Messaging Fees charged by the network are too high. **1B)** Fees charged by my bank provider are too high. **1C)** Liquidity related costs for this business are too high. **1D)** Capital related costs for this business are too high. **1E)** Costs related to counterparty and liquidity limits, fails in STP and incorrect processing are too high. **2A)** There is a lack of information throughout the lifecycle of the payment. **2B)** There is a lack of enhanced data and incomplete transaction reference data creates problems to reconcile transactions. **2C)** There is a lack of visibility of transaction related costs, i.e. who has paid which fees to whom for validation of AML/CTF, counterparty risk, liquidity reporting and credit limit. **3A)** Do you believe that Blockchain/Distributed Ledger Technology could be deployed as the basis for a new generation cross-border payment network?

Table 3.3: Percentage of respondents that strongly disagree, disagree, are undecided, agree or strongly agree with statements describing costs, information provision and technology development (World Regions)

Statement	Europe			Asia & Africa			Americas		
	Disagree	*Undecided*	*Agree*	*Disagree*	*Undecided*	*Agree*	*Disagree*	*Undecided*	*Agree*
1A	20	34	45	28	24	48	4	44	52
1B	18	29	52	16	16	68	4	40	56
1C	13	22	63	12	16	72	12	32	56
1D	6	22	70	12	24	64	0	56	44
1E	11	9	79	12	8	80	16	24	60
2A	2	6	90	12	8	80	4	12	84
2B	4	6	88	12	8	80	4	12	84
2C	2	13	84	0	4	96	0	4	96
3A	20	43	36	12	28	60	8	28	64

1A) Direct costs for Messaging Fees charged by the network are too high. **1B)** Fees charged by my bank provider are too high. **1C)** Liquidity related costs for this business are too high. **1D)** Capital related costs for this business are too high. **1E)** Costs related to counterparty and liquidity limits, fails in STP and incorrect processing are too high. **2A)** There is a lack of information throughout the lifecycle of the payment. **2B)** There is a lack of enhanced data and incomplete transaction reference data creates problems to reconcile transactions. **2C)** There is a lack of visibility of transaction related costs, i.e. who has paid which fees to whom for validation of AML/CTF, counterparty risk, liquidity reporting and credit limit. **3A)** Do you believe that Blockchain/Distributed Ledger Technology could be deployed as the basis for a new generation cross-border payment network?

Regional differences between Users and Providers are analysed in more detail in Annex 3.2 (See Figures A32.1 to A32.9). We looked at the average response of different groups, as well as the standard deviation. On average, our findings are as follows. To the question relating to messaging costs being too high, most respondents agreed, but there is a large proportion of undecided. More American respondents agreed, with a larger variation in Asia and Africa. Users' views were also more dispersed compared to providers (Figure A32.1). The second question related to fees: a higher proportion of users agreed with the statement. American, Asian and African respondents were most unhappy with current fees, whereas in Europe we recorded the highest dispersion (Figure A32.2). Our third question explored as to whether liquidity related costs were being perceived as too high: American respondents had diverse views, whereas more respondents in Africa and Asia agreed.

While liquidity costs are generally perceived as too high by Users, Providers views were more varied (Figure A32.3). The next question related to capital costs being perceived as too high: the large majority of respondents agreed or strongly agreed with this view (Figure A32.4). We find more disagreement in views regarding costs related to counterparty and liquidity limits, less between users and providers, with providers being more undecided. However, overall less than a quarter of respondents disagreed or were undecided (Figure A32.5).

Views were very consistent regarding the lack of information throughout the lifecycle of the payment: this is one of the major perceived pain points and, interestingly, no respondent strongly disagreed with the statement (Figure A32.6). Similarly, there was very strong agreement with the statement that a lack of enhanced data and incomplete transaction reference data creates problems to reconcile transactions (Figure A32.7). There was also almost universal agreement with the question as to whether respondents believe that there is a lack of visibility of transaction related costs, i.e. who has paid which fees to whom for validation of AML/CTF, counterparty risk, liquidity reporting and credit limits (Figure A32.8).

Our final question asked respondents: "Do you believe that Blockchain/Distributed Ledger Technology could be deployed as the basis for a new generation cross-border payment network?" We found Users more supportive of this view, whereas answers were dispersed among Providers. European respondents seemed less enthusiastic about the ability of technology to improve cross-border payments compared to American, Asian and African respondents (Figure A32.9).

The on-line survey allowed us to identify, validate and rank the key pain points, as illustrated in Figure 3.4. The strength of problem has been categorised as the ratio of respondents who agreed with the proposed statement to those who disagree.

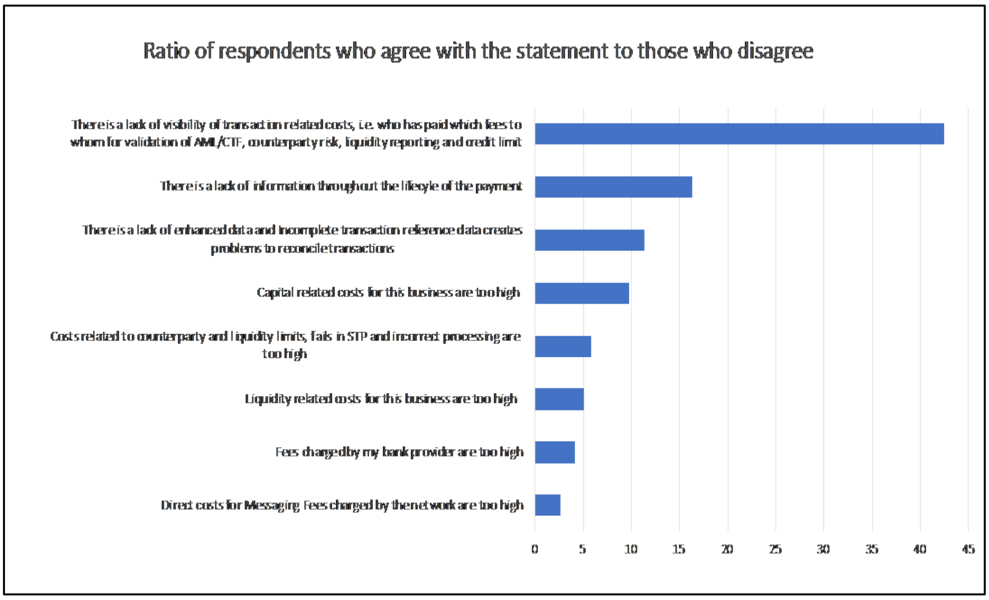


Figure 3.4: Pain points identification and ranking

As summarized in Figure 3.4, respondents felt the strongest about the lack of visibility of transaction related costs, followed by the lack of information throughout the lifecycle of the payment and lack of data and/or incomplete transaction reference data, which create problems to reconcile transactions. Interestingly the direct costs associated with messaging fees charged by the network were considered the least important.

From these results, it emerges than pain points related to information and transparency are even more relevant than cost-related frictions, such as liquidity and capital costs, costs for messaging fees and costs charged by Providers.

The survey results then constituted our starting point of discussion with the focus group, where the aim was to propose a potential approach to remove the identified pain points.

3.5.2 Focus groups

Following the results of the survey, we engaged in a number of focus group meetings. At the first focus group, held on the 15th of January 2018 in London, participants' views were sought on the survey results and the ranking of pain points and whether the latter was in line with the current observations on 'de-risking' in the market. The output of this meeting was an agreement on key requirements for an improved future of cross-border payments, as set out in Section 3.6.

The second focus group meeting was held on the 7th of March 2018, following a conference call held in February. This meeting focused on elaborating and discussing a set of potential design scenarios for the future of cross-border payments with the objective to align as much as possible with the set of key requirements that had been previously identified. As a second step the group also discussed a number of areas that could be improved through policy, regulation and standards with a particular view on the regulatory challenges associated with cross-border payments. The output of these discussions has been used as a basis to develop Section 3.7.

3.6 KEY REQUIREMENTS FOR A FUTURE CROSS-BORDER CORRESPONDENT BANKING PAYMENTS MODEL

Building on the identified shortcomings and pain points from an industry practitioner point of view, the first focus group session developed a set of key requirements that a future cross-border payments model would need to be able to satisfy.

Based on the experiences of the financial crisis of 2008/2009, when the lack of transparency on where market liquidity actually was, combined with a significant shortage of liquidity supply, an overall need to enhance financial stability in this space became apparent. Against this broader background the discussions of the focus group arrived at the following key success criteria for a sounder and more efficient future cross-border payments model.

3.6.1 Key Requirements

1. Settlement (including synchronisation)
2. Liquidity efficiency
3. Availability (technical access and uptime)
4. Ubiquity (relevant connectivity between systems and players)
5. Transparency
6. Predictability
7. Interoperability of systems

We will discuss these key requirements in detail below. In addition, focus group participants recommended that particular attention should be paid to policy, standards and best practice in the industry, so as to achieve a blueprint for a substantial improvement in cross-border wholesale payments.

3.6.1.1 Settlement (including synchronisation)

Settlement of transactions with finality is a key requirement in order to mitigate credit risk. Settlement can occur in commercial bank credit as well as central bank money, which have different risk factors as previously discussed. Irreversibility of transactions and legality of settlement is generally determined by law. The recommendation here is that for significantly high value transactions, settlement in central bank money should be the preferred option from a financial stability perspective. This would exclude transactions across an individual FI's own network.

In the context of emerging technologies such as DLT one of the central questions to address is 'how to create both Payment versus Payment (PvP) and Delivery versus Payment (DvP) outcomes in this new environment, i.e. atomic settlement' via code, rather than law'. The early conversations around 'synchronisation' are starting to point in that direction.[22]

3.6.1.2 Liquidity efficiency

Managing the balance sheet cost of supporting payment flows through efficient use of collateral/cash to safely process payments is a crucial requirement for an improved global cross-border payment process. Liquidity management tooling and cash/collateral movement would be features that enhance a commercial bank's ability to manage liquidity. Transparency of participants' balance sheet exposures at any point in the chain should be a key priority for banks. Furthermore, in

[22] Synchronisation in this context is the concept of a payment (or group of payments) settling if and only if another payment (or set) also settles (Bank of England, 2018).

order to reduce exposures between commercial parties and resultant cash/collateral needs, whether bi- or multilateral, netting solutions have the potential to support efficiency of participants across payments and FX. An example would be intra-asset class netting (e.g. euro, sterling etc.) but essentially this could include any product where a payment is required for settlement. This would implicitly add some delay in the transaction against the benefit of reducing cost and counterparty risk.

3.6.1.3 Availability (technical access and uptime)

This requirement is essential in order to make payments as relevant systems – messaging, internal bank systems, CLS, etc. – will need to operate properly and safely. In the scenarios developed in Section 3.7 availability will indicate the live status of the respective scenario (that is, the technology/system is available today, at least in some form, rather than being potentially available in the future).

3.6.1.4 Ubiquity (relevant connectivity between systems and players)

Connectivity is at the heart of a network industry such as payments. This criterion looks at the existing network of connected parties and the network dependencies, as well as the ease of connection to additional parties (e.g. scalability and potential access), including other networks or DLT like structures.

3.6.1.5 Transparency

This key requirement considers primarily the traceability of transactions, complemented by data around fees. The relevance of transparency as a key requirement was also evidenced in our empirical questionnaire, as respondents indicated that frictions around information and transparency were considered the most relevant pain points (see Section 3.5.1).

3.6.1.6 Predictability

In line with the empirical questionnaire results this requirement considers service-level agreements (SLAs), rulebooks and process timescale-guarantees that enable certainty of sufficient data to facilitate automated reconciliation and postings. This implies operation and technology stacks at any end point to handle the transactions quickly, automatically and at any time of day.

3.6.1.7 Interoperability of systems

To reduce fragmentation, complexity and associated costs and risks, a long-term goal is to improve interoperability between Payment Market Infrastructures (PMIs) and FIs, with a view to supporting convergence on the global ISO 20022 standard, which enables the exchange of larger data sets in a more harmonised way.[23] This will also help mitigate risks around AML/KYC/CTF and reduce the occurrence of exceptions and transaction fails.

---

[23] ISO 20022 is the international standard that defines the ISO platform for the development of financial message standards. Its business modelling approach allows users and developers to represent financial business processes and underlying transactions in a formal but syntax-independent notation. The first focus of ISO 20022 is on international (cross-border) financial communication between financial institutions, their clients and the domestic or international 'market infrastructures' involved in the processing of financial transactions. (https://www.iso20022.org).

3.6.2 Policy, standards and best practice

Beyond these criteria, the overarching objective of a future blueprint for correspondent banking transactions is to support financial stability and increase trust and direct communication between FIs around the world, such that more customers and markets can be reached. In addition, a more efficient way to manage regulatory risk across KYC/AML/CTF and sanctions related assurance, as well as cyber resilience, will need to be addressed with the help of policy, standards and best practice recommendations. These will be elaborated further in Section 3.8.

Future cross-border payments models also need to consider the FIs' challenge to replace, interoperate with, or reuse infrastructure at a time of increasing costs and reducing competition. The complexity and risk of wholesale systemic change is high and new models will need to take into account prolonged coexistence of traditional technologies and approaches. Furthermore, various central banks around the world are working on renewing their payment system infrastructure; for example, the Bank of England's RTGS renewal program; the new Canadian high value payment system; Australia's New Payment Infrastructure, amongst others. A big ambition in all of these system upgrade initiatives is the perspective of potential future cross-border coordination and interoperation between for example central bank RTGS systems.

In some regions of the world, the problems of 'de-risking', cost and lack of speed in cross-border correspondent banking and/or the desire to promote inter-regional trade leads central banks to step in and provide a connection to non-domestic/regional FIs (e.g. Gulf States). Whilst this has been perceived as a challenge by FIs in terms of removing the specific income stream associated to this business, future opportunities for FIs are in the area of data driven value-added solutions.

As these forces of change transform the commercial model for banks in the correspondent banking business, it can be expected that the transaction fee model will be further simplified with a view to removing deductions and that over time value-added and data centric pricing models will come to the fore.

The evolution of cross-border payments will also need to consider the reality of the payment markets moving into the 'real time' space. With the expectations of end users moving to a near real time service provision, the current trend in retail payment systems becoming near-real time is poised to become the norm in the future. There is rapid growth of Faster/Immediate Payments in many countries, filling the gap between traditional ACH and RTGS systems and perhaps constituting the beginning of a potential merging of Faster/Immediate Payment Systems and RTGS Systems.

A challenge for banks will be the fact that they usually don't have 100% real time availability of liquidity but instead manage their liquidity to the minimum necessary to cover for the payments they make. Liquidity has a cost to providers and hence any increase in the amount needed will drive up costs for banks and therefore users. Real time payments, where payments include final settlement, require greater liquidity as there is limited opportunity to smooth peaks and troughs of demand through netting and offsetting. As the boundaries between wholesale and retail payments continue to blur, and the future of real time unfolds globally, real time intraday liquidity management will become the central building block to make this business safer and more efficient. And as long as liquidity costs are below potential banking charges, the market is poised to become more efficient.

Let us now move into a set of examples, reflecting existing and future cross-border payment design models and see how far these can respond to the identified challenges, requirements and trends in the market.

3.7 DESIGN SCENARIOS FOR AN IMPROVED CROSS-BORDER PAYMENT PROCESS

Our main objective is to propose a blue print to take correspondent banking into the digital age. This can translate either into a new model altogether – i.e. correspondent banking arrangements will be replaced by something else – or it can represent changes to the way correspondent banking works today, for example in relation to the messaging system/type/content, the introduction of utilities etc.

In this section, we will explore alternative cross-border payment design models, existing models and emerging ones, as well as potential/theoretical scenarios.[24] We will then assess these scenarios in terms of how well they would address our set of requirements. Our evaluation of these models will also consider the need for practical feasibility, stakeholder buy-in and execution viability to actually implement these changes in the near to medium-term future. Ultimately, we aim to propose solutions that can have a meaningful and practical impact on the way the industry operates.

[24] Other use cases, in particular specific providers and their solutions/networks, have not been explored in further detail in order to avoid competition issues. In addition, the experiments by SWIFT of using DLT have not been included specifically as these only related to the specific area of supporting nostro-vostro account reconciliation.

Scenario 1	SWIFT Global Payments Innovation (gpi)
Scenario 2	A ‘narrow’ Clearing Bank
Scenario 3	Interconnected Automated Clearing Houses
Scenario 4	Integration of regional RTGS Systems
Scenario 5	Global Settlement Utility Model
Scenario 6	Synchronisation and Interconnectivity of RTGS Systems
Scenario 7	gpi Next Generation

Table 3.4: Design scenarios for cross-border payments

In the remainder of this section, we will review these scenarios in detail, and highlight pros and cons.

3.7.1 Scenario 1: SWIFT Global Payments Innovation (gpi)

The recent launch of the SWIFT Global Payments Innovation (gpi) solution shows that some of the drawbacks of the current system of correspondent banking can be removed by collaboration, business rule discipline and a willingness of FIs to deliver improved services for end-users.

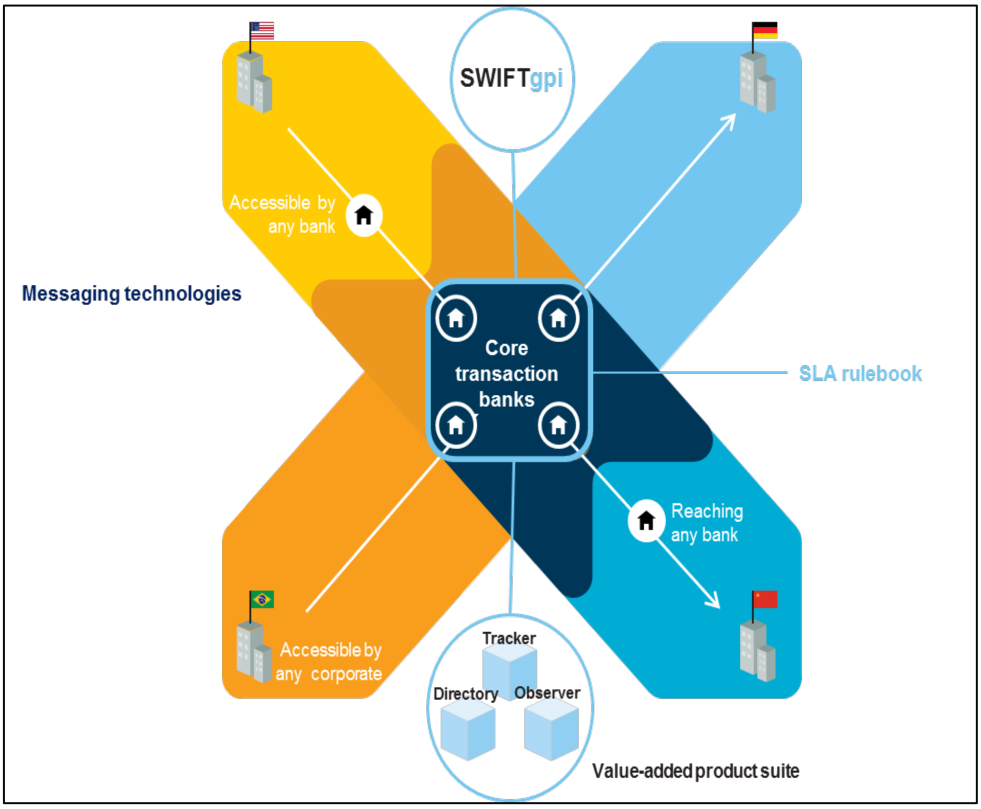


Figure 3.5: GPI model (source: SWIFT)

With the objective of reducing friction and enabling FIs to work better together, gpi provides a cloud-based service, accessible via APIs or MT199 messages, which allows FIs to track their payment transactions in real time by deploying the Unique End-to-End Transaction Reference (UETR) for every gpi transaction. The transparency along the chain around payment fees and final payment amount that will reach the beneficiary, along with the commitment by beneficiary institutions to credit – within their time zone – the beneficiary same day, supports payment users in better managing the accounts payable component of their company's working capital equation. Those FIs and PSPs participating in gpi start to see significant reductions in their payment enquiry costs, as counterparties now first consult the payment status in the cloud. There is also an enhanced perception by customers, as they receive an improved service for cross-border payments. Correspondents are now increasingly being asked to provide their ‘gpi compliance score’ by potential customers.

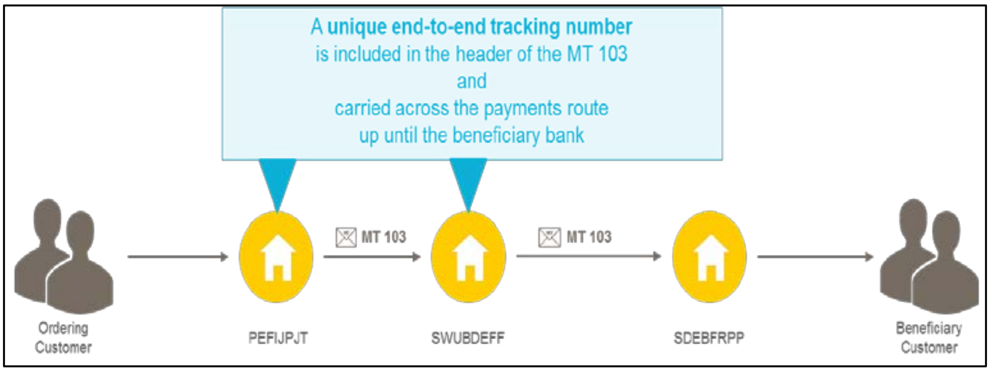


Figure 3.6: Illustration of UETR (source: SWIFT)

Thus far more than 180 banking groups of the roughly 3,000 banking groups on SWIFT have signed up to gpi, including 49 of the top 50 institutions in terms of value of transactions processed. 62 FIs are live with gpi as of May 2018. gpi payments cover more than 450 country corridors and represent a value of over 100 billion USD per day, or 25% of SWIFTs total cross-border payments in over 120 currencies. In order to achieve the strategic objective of extending gpi to all cross-border payments on SWIFT by 2020, the large clearing providers will need to bring their own global branch networks into gpi. In addition, smaller or more occasional users will need to implement a basic gpi service where the outcome of a cross-border payment is provided to the gpi tracker.

Despite the absence of an empirical market benchmark around pre-gpi speed of cross-border correspondent banking payments, there is a perception that transactions have become faster due to the peer pressure resulting from the transparency of the tracker. In addition, there is a requirement in the gpi SLA that payments are credited same day (depending on cut off times).

While for some banks this is not a challenge, others had to make changes to their daily operations in order to be able to conform to the gpi SLA. To complement the gpi rulebook and tracker, the ‘gpi Observer’ provides the critical success ingredient by objectively measuring gpi participants' compliance against the gpi rulebook. gpi statistics now indicate that almost 50% of gpi payments result in a credit to end-customers within 30 minutes, with 90% of gpi payments being credited within 24 hours. For the remainder, the reason for delay can objectively be attributed to particular regulatory and compliance requirements, such as extra document checks and local FX controls.

From a financial stability perspective, it is important to mention that a correspondent banking payment message is only passed on to the next bank in the chain once the relevant *Nostro*/*Vostro* balances have been updated, i.e. each bank has to settle its position with the previous bank in commercial bank credit. In response to demands of major cross-border banks for gpi support by market infrastructures (MIs) such as Fed, CHIPS and TARGET2, relevant steps were taken in 2017. Since mid-2018 58 SWIFT-based market infrastructures are able to clear gpi payments; 20 more SWIFT-based MIs a able to transport the UETR (and become full gpi if interested) as of November 2018, and local gpi market practices for Fedwire (USA), CHIPS (USA), CIPS (China), SIC (Switzerland) and FXYCS (Japan) have been made available (3 used in production), allowing the gpi to cover at minimum the top 10 currencies used for cross-border payments.

Since 2018, following the next annual SWIFT Standards Release, generating, passing on and receiving the UETR has become a compulsory requirement for all SWIFT users. This permits gpi customers to track any gpi transaction they are party to from an end-to-end perspective, unlike the previous situation where the gpi message flow stops at the non-gpi FI in the chain.

This also enables those non-gpi FIs and PSPs to immediately adopt the UETR as the de-facto Esperanto language for enquiries and investigation events such as AML/CTF requests or requests for information, supporting all players in improving their risk management capabilities. FIs are exploring innovative ways to use the cloud database, for example in order to reconcile their own transactions with their own transaction records. From 2020 all SWIFT FI users will have to provide a mandatory end beneficiary credit confirmation.

Moreover, as part of planned improvements gpi will include the ability for gpi-enabled FIs to immediately stop and recall a payment, irrespective of where this payment is in the gpi-inter-bank chain. This is a vital feature in the fight against fraud as well as error management. In addition, the transaction's progress on FIN will also be tracked, helping the FI beneficiary of the cover to track whether the cover was initiated – which is particularly useful from a counterparty risk perspective (tracking of cover launched in November 2018; tracking of institutional payments is to be confirmed).

In sum, the gpi scenario does address some of the key pain points expressed by market participants, which means that our recommendation is for participating FIs in correspondent banking to embrace and implement gpi to their own benefit and to the benefit of their clients. SWIFT gpi does not require structural changes to the current correspondent banking *Nostro*/*Vostro* account-based model and has a value and technology roadmap to help the community address the fundamental challenges of cross-border payments, as opposed to models introducing disruptive technologies and thus requiring banks to rethink and replace their front-to-back office infrastructures.

Settlement	gpi is only a messaging solution and does not deliver settlement. However, it does support transparency and risk management in commercial credit settlement.
Liquidity Efficiency	gpi reduces payment delays and thus can improve liquidity efficiency.
Availability	Yes
Ubiquity	Limited to SWIFT users and their clients.
Transparency	Yes
Predictability	SLAs and Rulebooks deliver key improvements. More work is on-going to deliver 'up front transparency'.
Interoperability	gpi is technology agnostic. Once SWIFT messages move to ISO 20022, gpi will also become ISO 20022 compliant.

Table 3.5: Benchmarking gpi against key requirements

3.7.2 Scenario 2: A 'narrow' Clearing Bank

This scenario represents a pure clearing system, where a clearing bank – narrow bank - connects individual banks and corporates across countries and allows them to exchange funds in real time, leveraging the bank's messaging network. This scenario is already a live scenario in the UK[25] and even though it is currently restricted to the UK, we have listed this as a potential scenario as the ambition is to expand this model globally.

[25] Clear Bank, launched in 2017, is the UK's first new clearing bank in more than 250 years. It offers banking services to financial service providers, FCA-regulated businesses and FinTech.

Settlement is achieved in near-real time in commercial bank credit and all positions are pre-funded, such that counterparty credit risk is managed. Ultimate settlement in central bank money would happen through the RTGS system that the clearing bank is connected to (similar to other ACHs). From a financial stability perspective, as the Clearing Bank acts as a connection layer between corporates and banks on the one hand and clearing systems on the other, even if critical volumes of high value transactions were to be processed via the clearing bank, such an entity would not need to become an FMI governed by settlement finality legislation and subject to CPMI-IOSCO principles for systemically large FMIs.

From a structural perspective this model combines the features of traditional correspondent banking, i.e. banks holding *Nostro*/*Vostro* accounts, and centralisation (i.e. banks connecting to the central clearing bank), which achieves the outcome of seamless STP. Additional services and functionality, such as KYC/AML/sanctions checking could be built on top and messaging should be based on IS0 20022 standards to enable global alignment and facilitate the use of a larger data set in order to improve predictability and transparency as well as reconciliation. For banks not directly connected to the clearing bank, there is the option to indirectly connect via entry point banks, which means that the service is likely to be slower than real time. In addition, institutional end users, such as corporates, would have the option to directly connect to the clearing bank, resulting in a shorter end-to-end payment chain and lower associated operational and regulatory risks.

Whilst the solution provides commercial money settlement, the liquidity and settlement dimension could become more challenging as higher value transactions start to be processed in this way, given both the need to pre-fund and the fact that per transaction settlement does not occur in central bank money.

At a structural level, this scenario flips the traditional correspondent banking *Nostro/Vostro* model on its head by replacing the inter-bank account chain with a direct FI or corporate to clearing bank connectivity via Nostro/Vostro accounts. Hence this scenario is disruptive but may in practice be complementary to correspondent banking cross-border payments. The success of this model depends on the extent to which there is network adoption. This is likely to be a challenge, as would be costs arising from KYC/AML risk management, in particular if it were to operate at a cross-border level. The difference to traditional ACHs competing for market share lies in the fact that the narrow bank acts as an aggregator that provides access to clearing, rather than being an ACH itself. Whilst this solution is limited to a domestic scenario today, the objective is to expand this to the cross-border space, i.e. potentially expand the connection to other ACHs.

Settlement	Yes, but only in commercial bank credit; deferred net settlement in RTGS system (BoE).
Liquidity Efficiency	From a liquidity perspective pre-funding could be costly unless FIs have efficient intraday liquidity and credit management processes in place. Netting will only become efficient if this gets broad adoption.
Availability	Yes.
Ubiquity	Subject to adoption levels; no international level.
Transparency	Yes.
Predictability	Rulebook based but possibly less predictable than gpi.
Interoperability	Yes as based on ISO 20022.

Table 3.6: Benchmarking a "narrow" clearing bank against key requirements

3.7.3 Scenario 3: Interconnected Automated Clearing Houses (ACHs)

Rather than having one and the same clearing bank facilitating real or near-real-time-cross border payments, a more complex but also more network-effect friendly way would be the interconnection of national ACHs, reflecting an increasing number of those already operating in a near real-time environment today (showing the blurring of ACH and Faster/Instant Payment Systems). Examples of this exist, e.g. in Europe where we have an interlinking of ACHs under the EACHA – the European Automated Clearing House Association – Framework, which connects 27 member institutions across SEPA on the basis of the international ISO 20022 messaging standard. In this regard it is important to remember that the SEPA scheme rulebooks, covering credit transfers and direct debits in euro, still reflect a lack of harmonisation, given the many options for banks and communities to define different approaches, e.g. in relation to remittance data and associated field structure, etc.

Mexico on the other hand has created a hybrid structure by interlinking its domestic RTGS system to the United States ACH (NACHA), enabling cross-border payments between these two markets.

At a global level, we have the example of the International Payments Framework Association (IPFA), a global interoperability scheme rulebook for cross-border retail payments, based on the ISO 20022 standard, similar to SEPA. This scheme leverages the existing correspondent banking network for cross-border low value transactions and payment aggregators deliver retail transactions via the different bank accounts they hold across more than 60 countries, often relying on the existing local payments infrastructures. This has ceased operating in 2018 however.

The difference between this model and the clearing bank model is reflected in the need to have an overall interoperability scheme rulebook, complemented by harmonised messaging standards. At the same time, end users are usually not directly connected to the respective local ACH, which means that the payment chain would be longer and more complex compared to the clearing bank scenario. In the case of IPFA, the reliance on the underlying inter-bank 'rails' indicates the dependency on correspondent banking.

Overall, the Clearing Bank and ACH interconnectivity models have limited application in the context of managing settlement risk in the high value cross-border inter-bank space. ACH transactions are not immediate and irrevocable in all instances and systems usually have transaction amount limits.

Settlement	Settlement in commercial bank credit; deferred net settlement in RTGS
Liquidity Efficiency	Cross-border netting capability (tbd)
Availability	Yes for EACHA; IPFA closed down in 2018
Ubiquity	Inter-ACH connectivity difficult and not proven at scale in cross-border context. SEPA/EACHA is most significant example in Europe
Transparency	No tracking, unless based on gpi
Predictability	Yes, rulebook based (e.g. SEPA, IPFA)
Interoperability	Would need to be ISO 20022 based (SEPA, IPFA are)

Table 3.7: Benchmarking interconnected ACHs against key requirements

3.7.4 Scenario 4: Integration of regional RTGS Systems

A parallel approach at the wholesale payment level would be to directly connect national RTGS systems with each other, creating almost an analogy to commercial banks being connected to each other via correspondent banking.

Such a model is currently in rollout mode across six countries in the Middle East under the Cooperation Council for the Arab States of the Gulf (GCC). The connection of the six Gulf state RTGS systems across Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the United Arab Emirates has been established on a legal basis, with the objective of supporting economic development and trade within the region. This will address the issues of end-to-end costs for users and the time taken from initiation of a payment to final delivery.[26]

Whilst the participating countries have not created a monetary union with a single currency, five out of the six countries have had a fixed peg to the USD for many years with Kuwait having a peg against an undisclosed basket of currencies, where that basket is assumed to be heavily weighted by the USD.

Many of the USD intra-GCC payments executed today start life as a debit to a local currency account of the sender, are then converted to USD, remitted as USD and then converted back from USD to local currency in order to credit the account of the receiver. There are also a number of pure USD-to-USD intra-GCC payments debiting and crediting USD accounts. An underlying rationale for the Gulf-RTGS initiative is represented by the objective to reduce the power of the USD as a reserve currency, given the nature of its risk profile and regulatory burden.

The Gulf model provides a central "Uber"-RTGS system, which links all participating RTGS systems and thus provides a full cross-border

[26] The integration of regional RTGS system is not unique to the Gulf, there are other examples among African states, for example between Kenya and Uganda.

RTGS solution. The domestic RTGS systems in the region have accounts in each other’s books, enabling transactions via the system to settle immediately with finality in central bank money. This will provide financial stability.

Central banks will deal with each other at a daily fixed currency translation rate. The reserve management operations of each participating central bank can decide whenever they want to settle or trade currency, or hold, or buy bonds etc. The central banks don't cover positions transaction by transaction; they will build up balances in each other’s books and will choose at intervals when to trade out these balances either to USD, their own currency or any other currency depending on their reserve management policy. Regulatory KYC and AML/CTF compliance responsibility for transactions settled in the RTGS remains with commercial banks.

Funds are co-mingled at FI direct participant level, meaning that domestic and cross-border liquidity is managed in the same pot, but is then being routed either nationally or cross-border. Enhanced liquidity management tools will be available, going hand in hand with the centrally aggregated liquidity. The list of eligible collateral is not the same across the different RTGS systems, which is an issue if it were to be a single standalone system. There is currently no netting foreseen, but this could be developed for the future.

The Gulf system is also being built for other countries to join if they wish to do so. It could ultimately provide settlement of a single Gulf currency in the region, if/once available. The new system will also support USD payments and the settlement agent for these transactions could be a commercial bank settlement agent but that is still to be resolved.

The Gulf example reflects the development from commercial bank correspondent banking to 'central bank correspondent banking'. In addition, it is a good example that shows that a monetary union is not a prerequisite to achieving a multi-country and currency RTGS.

However, the GCC model is very specific to this region and it is unlikely that this can be easily replicated at a global scale, given the legal, regulatory and political as well as standards and operational related challenges of alignment. Still, the formation of regional RTGS hubs should be encouraged with a view to creating interoperability bridges between the regions, which would allow for an increasingly global coverage.

Settlement	Yes, in central bank money
Liquidity Efficiency	Depends on Intraday Liquidity Savings Mechanism (ILSM). In addition, netting solutions could be added on top of the infrastructure
Availability	Not yet
Ubiquity	Good within the subset of participating RTGSs.
Transparency	Yes
Predictability	Yes
Interoperability	Will become ISO 20022 once participating RTGSs will switch to ISO 20022

Table 3.8: Benchmarking an integration of regional RTGS systems against key requirements

3.7.5 Scenario 5: Global Settlement Utility Model

Expanding the regional RTGS system hub creation – exemplified by the Gulf model - one could also consider the creation of a global market utility that facilitates settlement in central bank money by connecting country RTGS systems on the one hand and commercial banks on the other. At the same time optionality could be developed such that funds could either be settled on a net or gross basis. In addition, various value-added services could be connected to the market utility in order to allow for a platform approach, which would ultimately enhance competition and innovation as well. Services could include FX, information exchange – in particular intraday liquidity management related data – and netting and offsetting solutions. This could ultimately deliver a payments and settlement utility for global trade and trading.

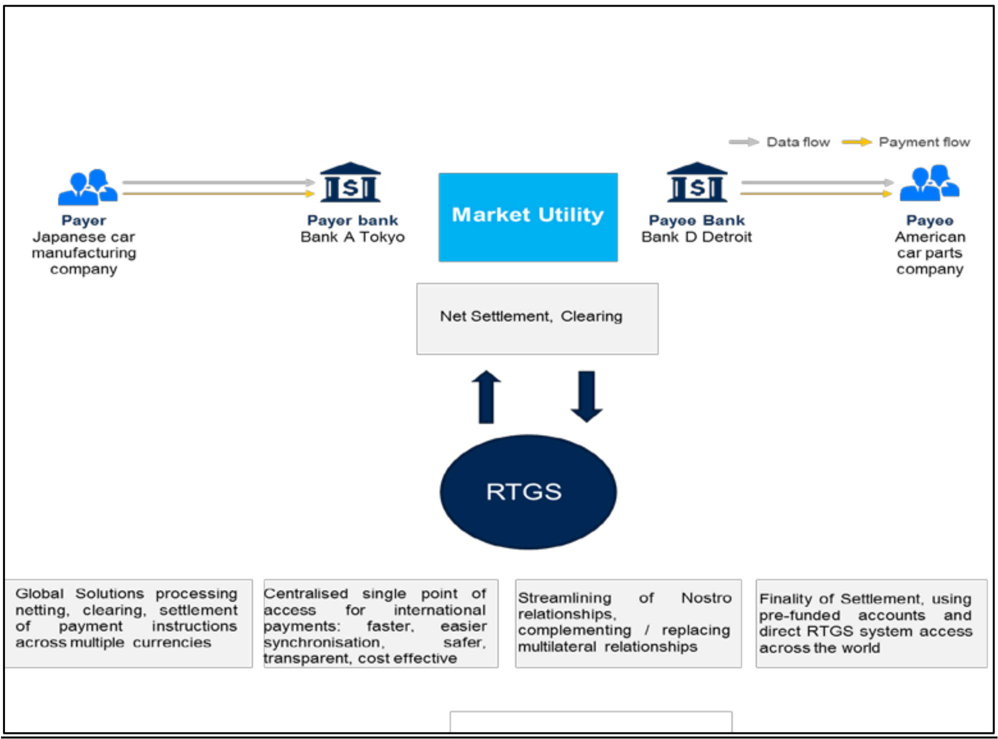


Figure 3.7: Cross-border Market Utility Model (source : R. Wandhöfer)

A global settlement utility should be developed in a way that would cover all of the identified requirements. However, its implementation would face a number of non-trivial challenges, ranging from network adoption to agreement on a common scheme rulebook and compliance with multiple regulatory regimes. The entity would have to be a regulated FMI under settlement finality legislation and in compliance with CPSS-IOSCO principles for systemically large FMIs. In order to manage the risk of 'too big to fail', specific contingency measures would also need to be put in place. Open questions include: "In what currency would settlement take place? Which FMI would ultimately manage and control the settlement? How would liquidity across the system be managed? Would the FMI be responsible for sanctions/AML/CTF etc.? In which currency would FIs have to fund their accounts with the FMI in? Would the FMI accept relationships with every bank globally and how would this be practically managed?"

Settlement	Yes; would need to be provided in central bank money
Liquidity Efficiency	Would need to offer multilateral netting solutions
Availability	N/A, but global infrastructure does exist for FX.
Ubiquity	Would be good within the participant subset
Transparency	Yes, this would be required
Predictability	Yes, SLAs and Rulebooks would need to deliver this (similar to existing global FX infrastructure)
Interoperability	Yes, it should be ISO 20022 and aligned with gpi

Table 3.9: Benchmarking a Global Settlement Utility model against key requirements

3.7.6 Scenario 6: Synchronisation and Interconnectivity of RTGS Systems

A variant of the global settlement utility model could be the deployment of the method of synchronisation, leveraging emerging (e.g. DLT) or existing technologies. Such a model is currently being discussed in central bank circles.

The objective is to create a 'third party provider model', where an RTGS system would have the functionality required for such a trusted third party, the 'Synchronisation Operator', to connect and offer synchronisation services to the market. The operator would have permission to earmark and transfer funds between participating institutions' accounts in the RTGS system, but would not hold an account itself. The service could be used by multiple Third Party Providers, and the functionality designed would be 'agnostic' to what the fund movements were being synchronised with, and so could be PvP or DvP, domestic or cross-border. In a cross-border context Synchronisation Operator(s) could be working with multiple national RTGS systems to synchronise cross border payments. Furthermore, the design of the RTGS system functionality could be agnostic to the technology used by the Synchronisation Operator. Therefore, no particular technology, for example DLT, would need to be deployed in order to make the model work, as it would be for the Synchronisation Operator to determine the appropriate method, technology etc. for delivering their particular service. Figure 3.8 below depicts the steps of synchronisation, provided by the Bank of England.

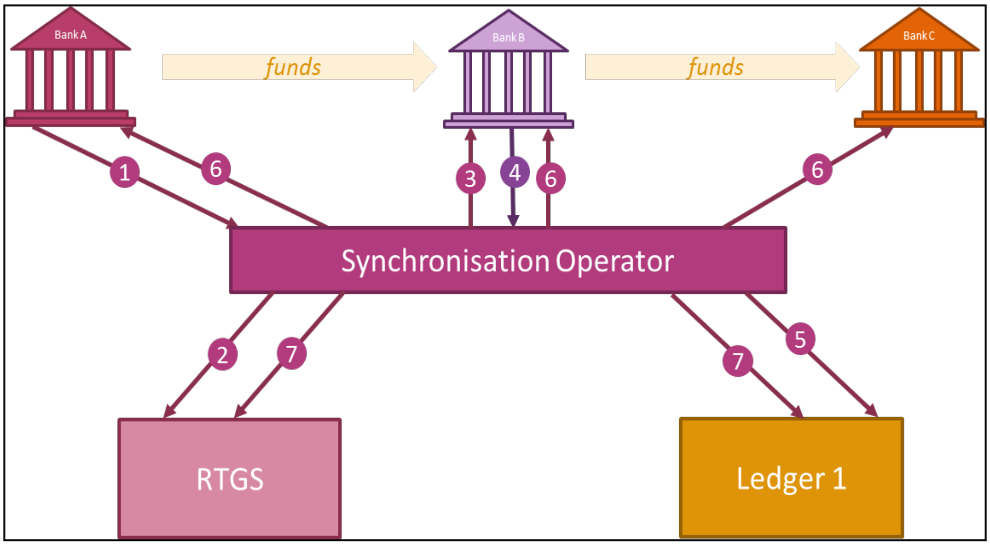


Figure 3.8: Synchronisation via RTGS System

(source: Bank of England)

1	Bank A notifies operator than it wishes to make a synchronised payment with Bank B in order to pay Bank C
2	Operator earmarks funds in Bank A's RTGS account
3	Operator notifies Bank B that funds are earmarked in RTGS
4	Bank B confirms that it is happy for funds to be earmarked in Ledger 1
5	Operator earmarks funds in Bank B's Ledger 1 account
6	Operator confirms to all parties that funds are earmarked
7	Operator simultaneously orders RTGS and Ledger 1 to release the earmarked funds to Bank B and Bank C respectively

The potential benefits of such an approach could be a simplification of some existing processes and the reduction of operational risk. There could be a reduction of credit risk by enabling DvP and PvP, whilst participants could avoid the need to prefund some large corporate transactions. Furthermore, this approach could lead to increased competition, particularly for new entrants, and allow participants to offer new products to new customers.

There are however also potential risks and challenges. For example, FIs are likely to want to retain control over payments (i.e. to have the option to stop a payment), particularly where large sums are involved. Earmarking of funds would have implications for managing available liquidity and may in practice not represent a performance guarantee in itself. Processes for 'exceptions' will need to be very clearly defined and the service functionality will need to be attractive enough to result in broader market adoption, which may be challenging if new technologies such as DLT are being deployed (due to migration complexity and potential associated costs). The Reserve Bank of Australia is already deploying synchronisation with regard to domestic housing transactions.

Building on the concept of synchronisation, design scenario 6 (see Figure 3.9) provides a perspective of how cross-border flows could be managed, by combining earmarking and synchronisation capabilities between central banks with the flow of correspondent banking payments.

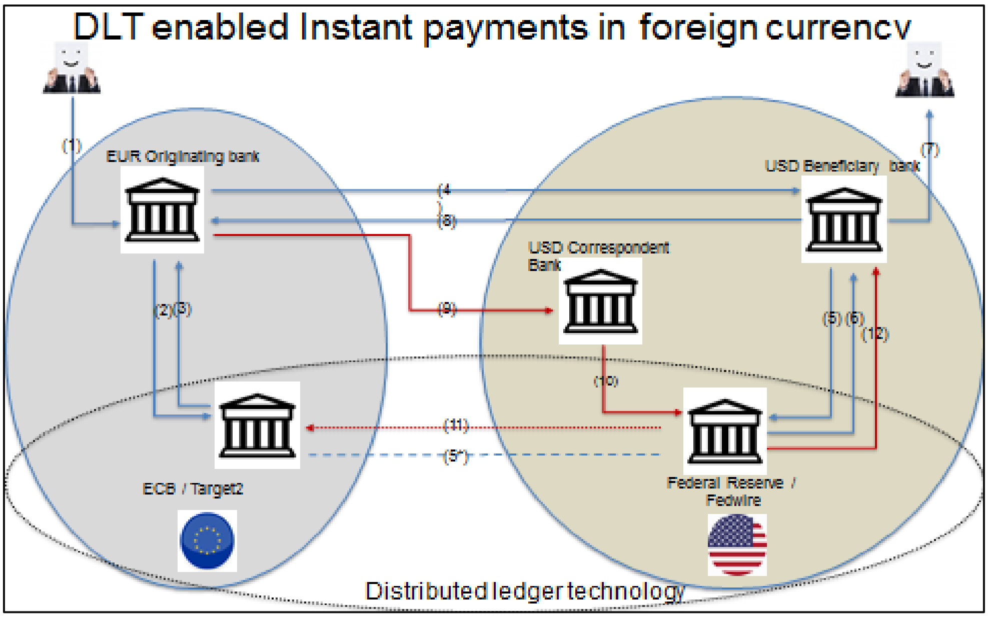


Figure 3.9: Global RTGS System interconnectivity (source: RedCompass)

In this model we chose to use a private distributed ledger model, where central banks connect with each other for purposes of earmarking funds. The abovementioned Synchronisation Operator would thus be represented by the DL itself in this example. Alternatives could also include leveraging the Utility Settlement Coin model (a DLT based wholesale digital currency), which would enable a more efficient flow of inter-bank balances held in RTGS systems. The transaction steps depicted in Figure 3.9 are as follows:

(1) Customer initiates a payment instruction in USD

(2) EUR originator bank makes a request to reserve USD for the transaction towards the ECB

(3) In case the ECB can reserve the funds on behalf of the EUR originator bank, it sends a positive acknowledgement – with a reservation ID

(4) EUR originator bank sends the payment message (credit transfer) to the USD Beneficiary bank, which includes the ECB reservation ID

(5) USD beneficiary bank validates the request and asks for a confirmation from the Federal Reserve if the payment can go through

(5*) The Federal Reserve confirms if the reservation at the ECB is guaranteed via the DL, which connects the two central banks

(6) The Federal Reserve informs the beneficiary bank that the payment can go through / is guaranteed

(7) The beneficiary customer is credited

(8) The EUR ordering bank receives the confirmation that the beneficiary has received the funds

(9) The ordering bank releases a 'cover' payment (e.g. MT202COV)

(10) The USD correspondent bank debits the *Vostro* of the EUR originator bank and settles the payment via Fedwire; the correspondent also provides the FX to the EUR originator bank

(11) The ECB (via the TARGET2 system) is informed that the reservation can be released, using DLT

(12) The USD beneficiary bank receives the funds

When discussing this scenario, several key questions and issues were identified. The objective of this scenario is to increase financial stability and lower the risks associated with commercial bank credit settlement for cross-border correspondent banking payments by leveraging central banks' support through earmarking. However, in the context of the current potential model for synchronisation, as explained above, earmarking funds may not be equivalent to extending a central bank guarantee. Synchronising the earmarking process with the actual payments flow in the correspondent banking space is a further challenge. Therefore, it is likely that liquidity risk would still be an issue for the beneficiary bank, i.e. in the situation where the beneficiary customer is credited before the beneficiary bank itself has received the funds from the correspondent bank (i.e. induced settlement risk). Additional questions around time zones and difference in value dating remain (e.g. the US to Australia corridor). It is equally unclear who would be responsible for sanctions screening in this model. Potential issues around application of funds, repairs, rejects and returns would equally need to be considered. Operations and reconciliation could potentially be streamlined using DLT, but technology alone cannot satisfactorily fix the set of identified issues in correspondent banking payments.

In a hypothetical future scenario, a potentially viable way to enable central bank money settlement for cross-border transactions leveraging DLT would be if central banks were to issue fiat currency on the DL and, via the establishment of Interledger protocols, provide central bank settled cross-border payments via atomic settlement.

However, such an approach could potentially have significant implications on the way the payment industry operates. Despite regional RTGS system hub initiatives, discussed in scenario 4, a large-scale approach of RTGS system connectivity via DLT deployment and issuance of Central Bank Digital Currency (CBDC) is an unlikely scenario in the short to medium term. As proposed by the Bank of England synchronisation model, other technologies could be explored for this purpose, allowing for ease of migration and adoption. Cross-border legal and regulatory questions as well as the extent to which such as solution could truly reduce inter-bank settlement and counterparty risk, would need to be tackled.

Table 3.10 summarises which requirements such a scenario is likely to be able to cover under the circumstances.

Settlement	Yes, in commercial credit, but with central bank earmarking support (guarantee?)
Liquidity Efficiency	No specific improvements unless gpi supports indirectly through predictability and transparency
Availability	N/A; DLT is not yet mature, and Interledger connectivity would need to be established
Ubiquity	This would be a key requirement to ensure reach
Transparency	Yes, this would be required
Predictability	Yes, a Rulebook would be required
Interoperability	Should be ISO 20022 based

Table 3.10: Benchmarking Synchronisation and Interconnectivity of RTGS Systems against key requirements

3.7.7 Scenario 7: gpi Next Generation

A final scenario, which we will call gpi next generation, looks further at reducing systemic risk in the critical area of inter-bank high value payments.

The aim of reducing settlement and counterparty risks in correspondent banking is being tackled from a gpi perspective with the roll out of the gpi Financial Institution Transfer (gFIT) service (date tbc.). In order to bring transparency and real time information to these critical high value transactions, the service will provide tracking of institutional payments (over FIN) by tracking MT 202 and MT 205 messages, followed by the plan to issue a rulebook for participants that will enable tracking of these transactions over non-FIN networks and market infrastructures. The rulebook will require FIs to confirm to the tracker once the beneficiary's Agents *Nostro* account has been credited, or flag any processing issues inside the FI, such that FI intraday liquidity management can become more accurate and reconciliations of payments can improve. This step, in combination with gpi-compliant infrastructure settlement in RTGS, would deliver significant benefit in managing systemic and counterparty risk, despite the reality of the continued practice of operating often undisclosed and uncommitted intraday credit lines – where these are ultimately more liquidity efficient than pre-funding of every transaction. This is likely to be the best possible outcome in light of the impossibility to establish harmonised bankruptcy laws across the globe that would otherwise define that positive funds held in *Nostro* accounts cannot be clawed back by the respondent FI (the User of correspondent banking services) in a scenario of intraday failure of such institution.

By 2022/2023 SWIFT is planning to migrate to the ISO 20022 standard, including gpi, which will allow parties to send more data in the payment message, allowing for more clarity on purpose of payment and the parties involved (including on-behalf-of payments). This will bring a substantial risk related improvement compared to today's MT messages, which are limited in the number of characters and often create AML compliance challenges for FIs. ISO 20022 will allow FI's to optimally include 'Know your Transaction' – KYT – data. This move also ties in with the increasing use of ISO 20022 in FMI/PMIs and will enable improved compliance in correspondent banking payments.

A planned 'pre-validation service' (for 2019 and beyond) will further support preventing STP and data gap related issues (e.g. missing clearing codes) as well as problems with closed or wrong beneficiary accounts down the payment chain. And finally, to complement a 'Case Resolution service' currently under exploration would further support FIs in the context of missing information in payments and specifically support sanctions related requests, given that sanctions information cannot be pre-validated at the start of a payment. This move would also support enquiries related to repairs, rejects, returns, and transactions that cannot be applied to an account. An important element here is that this service will directly connect banks that need to resolve issues rather than requiring them to go back through the banking chain. Furthermore, an audit trail of communication would be provided.

SWIFT has also experimented with DLT in the context of a Proof-of-Concept to deliver real time *Nostro*/*Vostro* account reconciliation. The exercise demonstrated that business requirements were met but point to the challenge of industry adoption, such as the prerequisite for FIs to move from batch to real-time liquidity processing and reporting as well as requiring IT back office upgrades.

It also showed that DLT is only one of several potential technologies that could be deployed, which indicates that technology itself is not the determining factor (SWIFT DLT PoC Findings, 2018). However, given the continued evolution of DLT it is recommended to investigate potential application of this technology further in the context of gpi.

Settlement	gpi is only a messaging solution and does not deliver settlement. However it will further support transparency and risk management in commercial credit settlement for high value payments
Liquidity Efficiency	gpi reduces payment delays and thus can improve liquidity efficiency
Availability	In future
Ubiquity	If on SWIFT network, limited to users and their clients
Transparency	Yes
Predictability	Yes, Rulebooks would be in place
Interoperability	gpi is technology agnostic. Once SWIFT messages move to ISO 20022, gpi will also become ISO 20022 compliant.

Table 3.11: Benchmarking gpi Next Generation against key requirements

3.7.8 Design Scenario Evaluation

In this section we discuss the results of our design development exercise. We have ranked the outcomes in line with the set of key requirements as defined in Section 3.6. To complement these practical design scenarios, we have also developed a set of policy recommendations (Section 3.8) that would be key enablers for delivering improved cross-border payments. Table 3.12 provides a ranking and high-level evaluation of the different cross-border payment design scenarios discussed in this Chapter with a particular view on time to delivery and associated effectiveness of the measure.

Ranking	Scenario	Commentary
1	gpi	Easiest to implement and impactful. Remaining settlement risk on clearing banks but increased adoption by FMIs, including RTGS systems would help end-to-end transparency. Limitation: to SWIFT users and their clients (but represent the majority of cross-border market players); importance of contingency/resilience of network and established multibank governance model.
2	gpi Next Generation	Potentially very impactful in terms of achieving messaging based transparency for high-value interbank transactions. Could meaningfully reduce settlement risk on clearing banks. Expected future benefits in the context of AML/CTF compliance and sanctions screening

		once those solutions will come into place. Limitation: to SWIFT users (but represent the majority of cross-border market players); importance of contingency/resilience of network and established multibank governance model. The planned move to ISO 20022 will further add benefits as discussed.
3	Regional RTGS system	Impactful in terms of financial stability but restricted to the region; very difficult and time-consuming to design and implement; disruptive impact on business models of traditional correspondent banks; potential to interlink regional hubs as they emerge (e.g. GCC with Eurozone)
4	Clearing Bank	Positive as it reduces the length of the interbank chain and hence complexity and risk; commercial bank credit settlement only and mainly focused on retail, low value transactions. As boundaries blur between retail and wholesale with high value transactions being managed in a low risk way, relevance could increase; needs network adoption and currency expansion; use of ISO 20022 positive.
5	ACH Interconnectivity	In place globally for some time with the IPFA scheme but little adoption (now decommissioned); commercial bank credit settlement only and main

		focus on retail transactions – once boundaries blur between retail and wholesale with high value transactions being managed in a low risk way, relevance could increase; use of ISO 20022 positive.
6	Market Utility	Whilst addressing settlement finality in central bank money, the utility could become too big to fail/centralising flows and risks; operational contingency important; question whether this should be a non-commercial FMI; governance/regulatory/investment challenge to set this up.
7	RTGS system Interconnectivity leveraging DLT/Synchronisation	Model discussed does not sufficiently address the market problems. Additional challenge of technology adoption of DLT and no clear picture as to how this could really improve financial stability and settlement finality, unless we move into a CBDC/CBCC and Interledger Protocol world. If everything becomes real time there is no possibility for liquidity optimisation as there is no ability to net. Synchronisation element looks theoretically promising but will require more in-depth development.

Table 3.12: Ranking and evaluation of scenarios

3.8 POLICY RECOMMENDATIONS

In order to complement the above design recommendations and with the objective of addressing the challenge of AML/KYC/CTF and sanctions in cross-border payments, the following actions are recommended.

First of all, for the purpose of ensuring a harmonised process of identification of payers and payees in a transaction and consistent with the views of the CPMI (CMPI, 2016) it is recommended to use the global Legal Entity Identifier (LEI) – a standard identifier for legal entities - in the payment message. Technology, in this instance DLT, could be used to broadcast the LEIs of participating institutions to the market. We already see LEIs being increasingly used with online digital certificates for additional verification of identity and business activity online.

As a complementary measure, the development of a second standard identifier for individuals could be considered, and this information could also be carried in the payment message. ISO might be an appropriate entity to look into such standardisation work, given the need for global consistency.

Furthermore, national regulators tend to require information on business, customer address, Business Identifier Codes (BIC), or bank account identifiers, tax identification numbers, etc. All of this information could be stored in a national KYC registry, which could serve as a golden copy for customer KYC data in that particular country – an approach that is also supported by the CPMI (CPMI, 2016). Note that various types of local and regional registry solutions have already started to emerge over the last few years (e.g. SWIFT registry, Nordic banks registry, Singapore etc.). Such registries would need to be continuously updated by banks with fresh information including fraud alerts and other relevant data.

One could even consider putting registries on a DL and allowing the government to validate LEI information. In order to establish the required legitimacy and effectiveness of use of such registries for the purpose of enhancing trust in cross-border payments, the Basel Committee in collaboration with the FATF could consider developing a set of key requirements that these national KYC registries would need to fulfil. Benchmarking alignment with these criteria could be performed via a peer review process, similar to the Basel Accord compliance peer review process, highlighting which countries have made the required efforts. The end goal would be that transactions between countries with 'reviewed and endorsed' KYC registries can flow more easily across borders, helping to support more trust between FIs. An essential item to address in all of this is legal liability for KYC in the context of outsourcing. Unless we have liability ownership of KYC utility (and other relevant compliance solution), we will continue to see limited success of those initiatives in bringing about the desired efficiency for this business.

A further measure, also endorsed by the CPMI (CPMI, 2016), could be an improved process of information sharing between FIs across borders, in relation to their due diligence and AML/CTF/KYC and sanctions related obligations. The challenge of FIs today is that local data privacy legislation and unclear messages from various national regulators make it difficult for FIs (which in some cases require due diligence information on their customers' customers – also known as 'KYCC') to share related information with each other. FATF clarified in October 2016 that FATF recommendations do not require FIs to conduct customer due diligence on the customers of their customer (KYCC). However, in cases where there is any unusual activity or transaction on the part of the respondent, or any potential deviations from the agreed terms of the arrangements governing the correspondent banking relationship, the FATF noted that, in practice, the correspondent institution will follow up with the respondent institution by making a request for information on any particular transaction(s), possibly leading to more information being requested on a specific customer or customers of the respondent bank. Information sharing is a key area that will need to be fostered further.

With a view on the regulatory and policy angle, cross-border payments of any kind would significantly benefit from a harmonised set of rules when it comes to the conduct of FIs/PSPs - as inspired by the European Payment Services Directive (PSD 2; Directive (EU) 2015/2366). In particular, the requirement of transparency around fees, deductions and FX rates applied as well as the prohibition to take float on incoming customer payments would have the potential to further enhance the practical messaging initiative of SWIFT gpi as well as to improve those payment transactions that remain outside SWIFT.

3.9 RESULTS AND DISCUSSION

In this Chapter we took a pragmatic approach to addressing the challenges surrounding cross-border correspondent banking payments. We engaged with practitioners to establish a set of agreed areas of challenge and associated design criteria. These have fed into the development of a set of design scenarios and options – some live and some planned or theoretical. We reviewed seven scenarios and evaluated the potential benefits and drawbacks of each.

3.9.1 Practical implications for the industry and regulators

Our results shows that gpi implementation by FIs has the potential to deliver more transparency to cross-border payments. This enhanced transparency, complemented by increasing predictability and discipline over time as additional rulebooks and SLAs are put in place, will be able to help institutions to better manage counterparty and financial stability related risks in the interbank space. Even though the risk associated to extending intraday credit to FIs will not be directly reduced via gpi, the transparency will help participants to see where the cover funding is in the payment chain and based on that information decide whether to pay out or not. The early visibility will allow any emerging problem to be tackled before it risks going out of control (i.e. avoid a Lehman scenario). Furthermore, we will have to be alert to the dynamics of peer group pressure and whether this transparency and predictability will encourage 'good' or 'bad' behaviour by institutions.

Regulators will play a key role in further promoting the adoption of ISO 20022 and the LEI as well as taking measures in support of the industry's ability to comply with AML/KYC/CTF (e.g. KYC registries), harmonisation of rules and provision of more clarity and encouragement for inter-FI information sharing. Based on experience, liability ownership of solution providers in the context of KYC utilities and other relevant solutions will be the only way to truly unlock the benefits of these solutions. This will need to be complemented by FIs taking active steps in addressing shortcomings in group level intraday liquidity management, both at the correspondent bank and user bank side.

3.9.2 Limitation and future research suggestions

We also highlight that the deployment of new technologies, such as DLT, is no panacea. Apart from the lack of maturity of this technology, there are only a few international bodies that have thus been successful in delivering distributed network management across a range of diverse stakeholders. Network governance is a key requirement that cannot be delivered by technology alone and there is a need – as identified and addressed by gpi – to deliver more SLAs and transparency between FIs.

Before we can consider moving into a new technology stack based on DLT, we will need to prove that the technology can work in the intended way and at a scale, and that the technical migration challenge is feasible for the size of the network we need to cover. This means that SWIFT should for example investigate further the technical side of DLT-based solutions in the context of the future evolution of gpi.

Future plans for central bank RTGS systems to leverage Synchronisation Operators to facilitate cross-border payment connectivity whilst delivering the financial stability benefit of settlement finality will need to be developed further, before any practical steps for implementation can be taken.

Annex 3.1: CROSS BORDER PAYMENTS INNOVATION QUESTIONNAIRE

ABOUT YOUR ORGANISATION

1. **Please indicate the type of organisation**

☐ Bank

☐ Non-bank

if "Non-bank" please indicate

☐ Payment services

☐ Other financial services (e.g. FinTech)

☐ Central Bank

☐ Other ________

2. **Which geography does your organisation cover? (Please tick as many as appropriate)**

☐ Europe

☐ Middle East

☐ Africa

☐ North America

☐ Latin America

☐ Asia Pacific

3. **Please indicate the country of your organisation (location of HQ)**

[dropdown list countries]

4. Is your organisation a SWIFT user?

☐ Yes

☐ No

5. Whilst most banks are both providers and buyers of correspondent banking services, please identify which is your PRIMARY focus:

☐ Provider

☐ User

ABOUT YOUR ROLE

6. Please indicate your job title
[free text]

7. Please indicate your job function (select the one where you spend most your time on)

☐ Network Management

☐ Cash Clearing Product Management

☐ Operations

☐ Product Development / Innovation

☐ Other, please specify: ___________________________

VALIDATION OF PAIN POINTS

8. As user and/or provider of correspondent banking services do you agree with the following pain points in the context of costs?

	Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
a) Direct costs for Messaging Fees charged by the network are too high	☐	☐	☐	☐	☐
b) Fees charged by my bank provider are too high	☐	☐	☐	☐	☐
C) Liquidity related COSTS For this business are too high	☐	☐	☐	☐	☐
D) Capital related costs for this business are too high	☐	☐	☐	☐	☐
E) Costs related to counterparty	☐	☐	☐	☐	☐

and liquidity limits, fails in STP and incorrect processing are too high					

9. As user and/or provider of correspondent banking services do you agree with the following pain points in the context of transparency?

	Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
A) There is a Lack of information throughout the lifecycle of the payment	☐	☐	☐	☐	☐
B) There is A Lack of enhanced data and Incomplete transaction reference data creates problems to reconcile transactions	☐	☐	☐	☐	☐

C) There is a lack of visibility of Transaction related costs, i.e. who has paid which fees to whom for validation of AML/CTF, counterparty Risk, Liquidity reporting and credit limits	☐	☐	☐	☐	☐

INNOVATION APPROACH

10. Is your organisation currently participating or planning to participate in any of the below SWIFT Innovation Initiatives? Please tick as appropriate.

☐ GPI

☐ DLT PoC Nostro/Vostro Reconciliation

☐ None

11. Do you believe that Blockchain/Distributed Ledger Technology could be deployed as the basis for a new generation cross-border payment network?

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
☐	☐	☐	☐	☐

12. Does your organisation experiment with or already deploy blockchain/Distributed Ledger Technology?

☐ Yes, please provide some high level detail on the area of application:

____

☐ No

13. Would you be available to be contacted in order to participate in our research?

☐ Yes

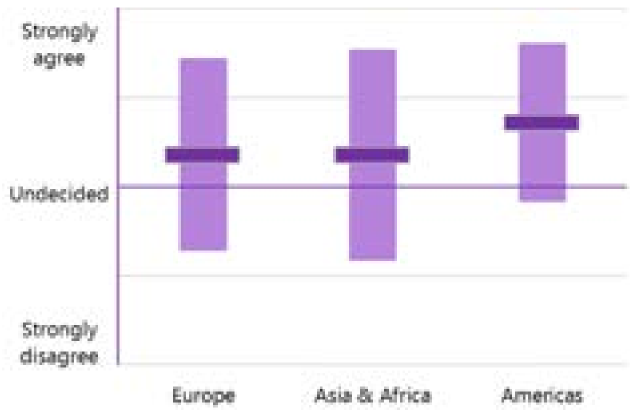
☐ No

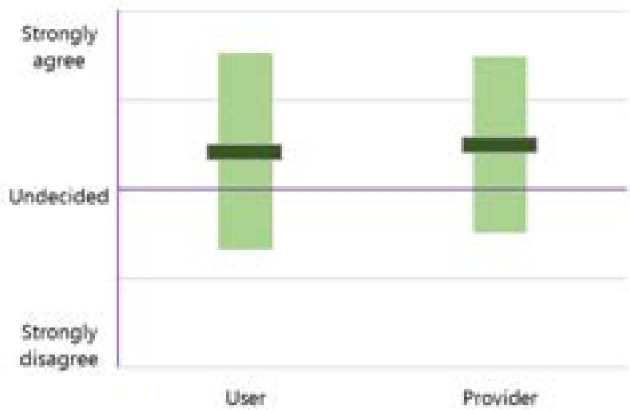
14. If yes, please provide your name, organisation, e-mail and/or phone number where we can contact you

[data fields]

Annex 3.2: CROSS BORDER PAYMENTS INNOVATION QUESTIONNAIRE RESULTS

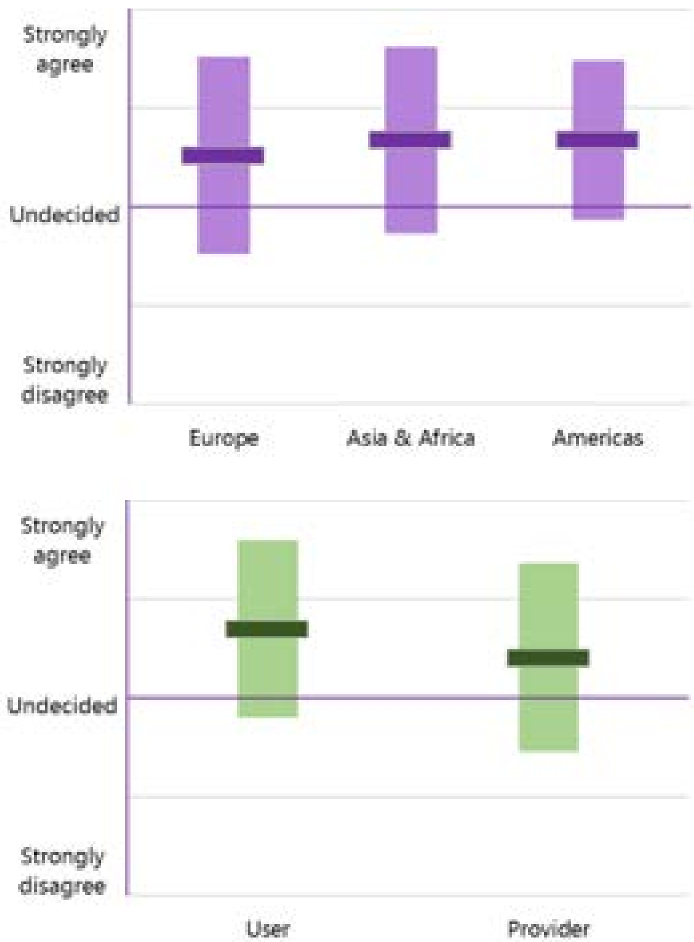
Figure A32.1: Direct costs for Messaging Fees charged by the network are too high.





Note: The figure depicts the answers to the question by distinguishing respondents according to their geographical location and whether their institution is a user or provider of correspondent banking services. The horizontal line indicates the average response, the vertical bar indicates the standard deviation,

Figure A32.2: Fees charged by my bank provider are too high.

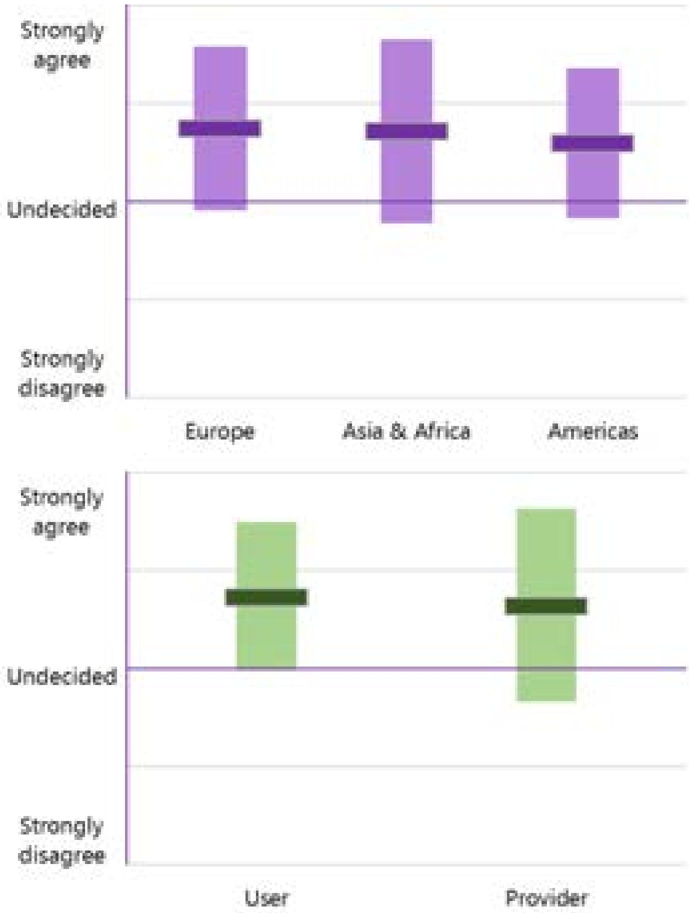


Note: The figure depicts the answers to the question by distinguishing respondents according to their geographical location and whether their institution is a user or provider of correspondent banking services. The horizontal line indicates the average response, the vertical bar indicates the standard deviation,

Figure A32.3: Liquidity related costs for this business are too high.

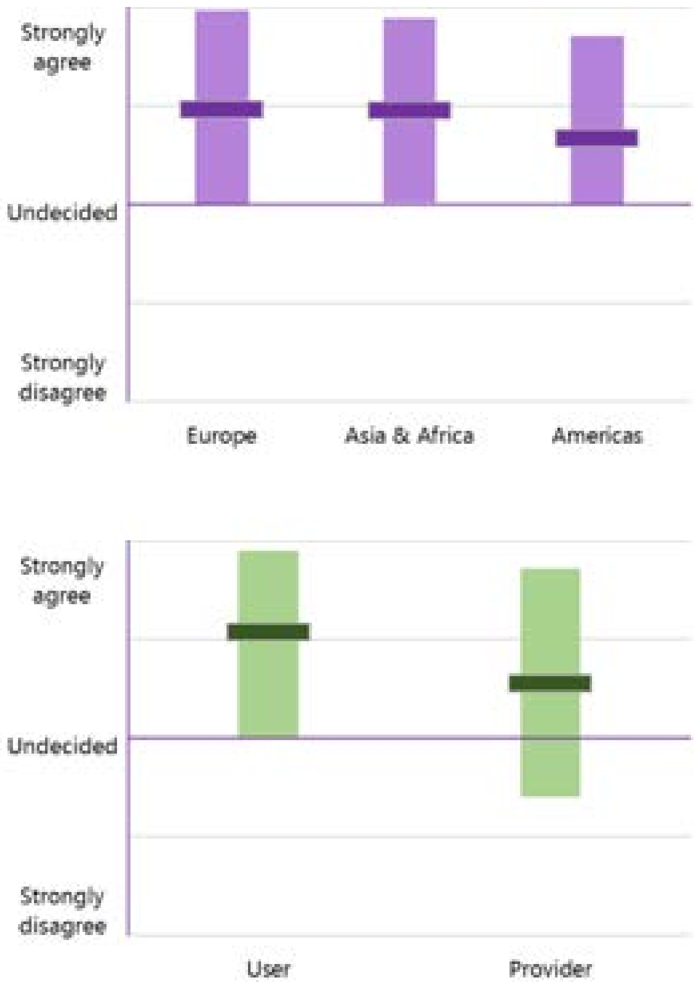
Note: The figure depicts the answers to the question by distinguishing respondents according to their geographical location and whether their institution is a user or provider of correspondent banking services. The horizontal line indicates the average response, the vertical bar indicates the standard deviation,

Figure A32.4: Capital related costs for this business are too high.



Note: The figure depicts the answers to the question by distinguishing respondents according to their geographical location and whether their institution is a user or provider of correspondent banking services. The horizontal line indicates the average response, the vertical bar indicates the standard deviation,

Figure A32.5: Costs related to counterparty and liquidity limits, fails in STP and incorrect processing are too high.

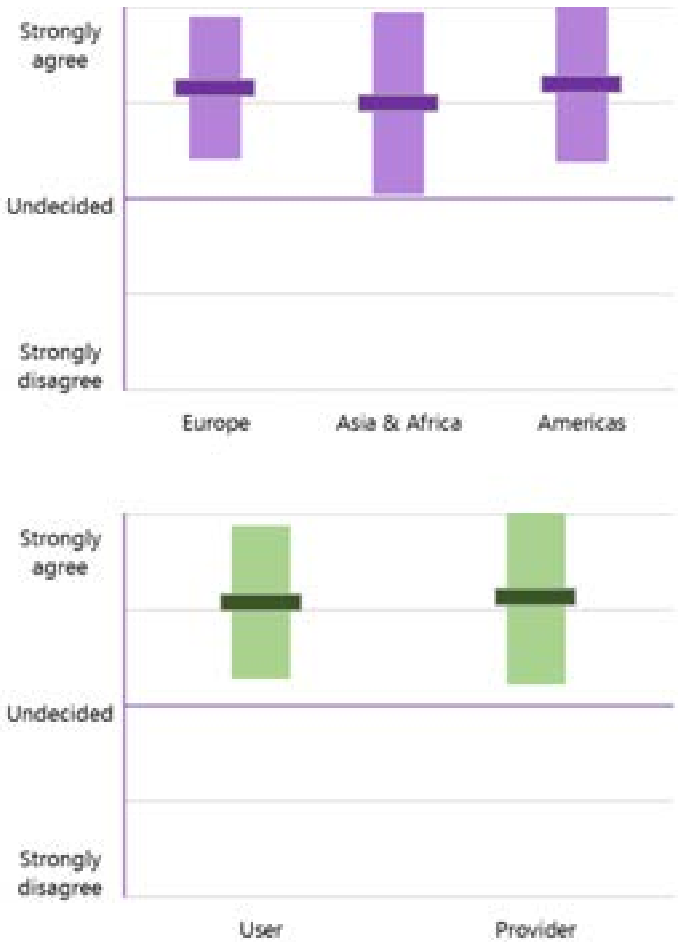


Note: The figure depicts the answers to the question by distinguishing respondents according to their geographical location and whether their institution is a user or provider of correspondent banking services. The horizontal line indicates the average response, the vertical bar indicates the standard deviation,

Figure A32.6: There is a lack of information throughout the lifecycle of the payment

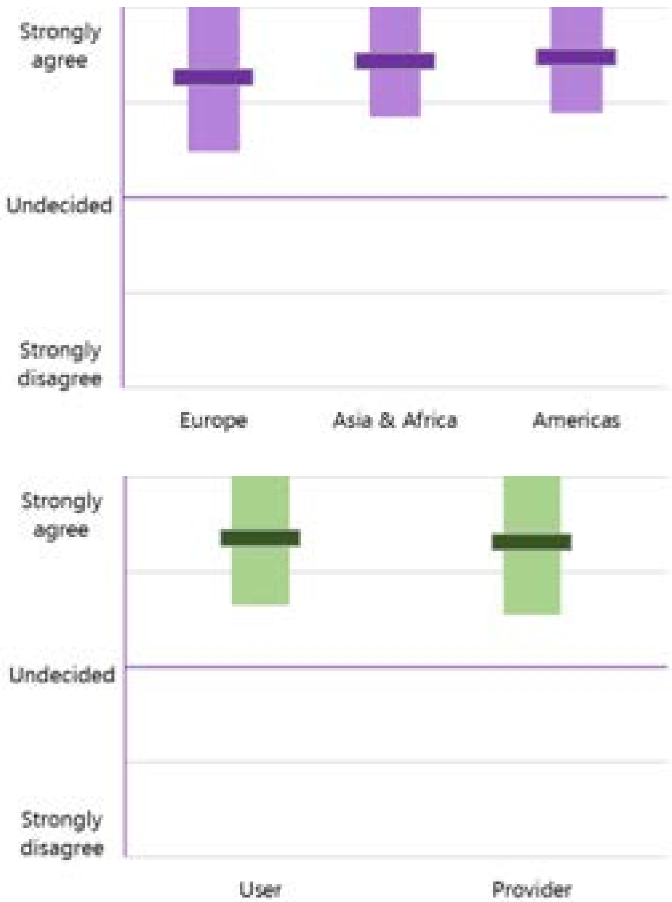
Note: The figure depicts the answers to the question by distinguishing respondents according to their geographical location and whether their institution is a user or provider of correspondent banking services. The horizontal line indicates the average response, the vertical bar indicates the standard deviation,

Figure A32.7: There is a lack of enhanced data and incomplete transaction reference data creates problems to reconcile transactions.



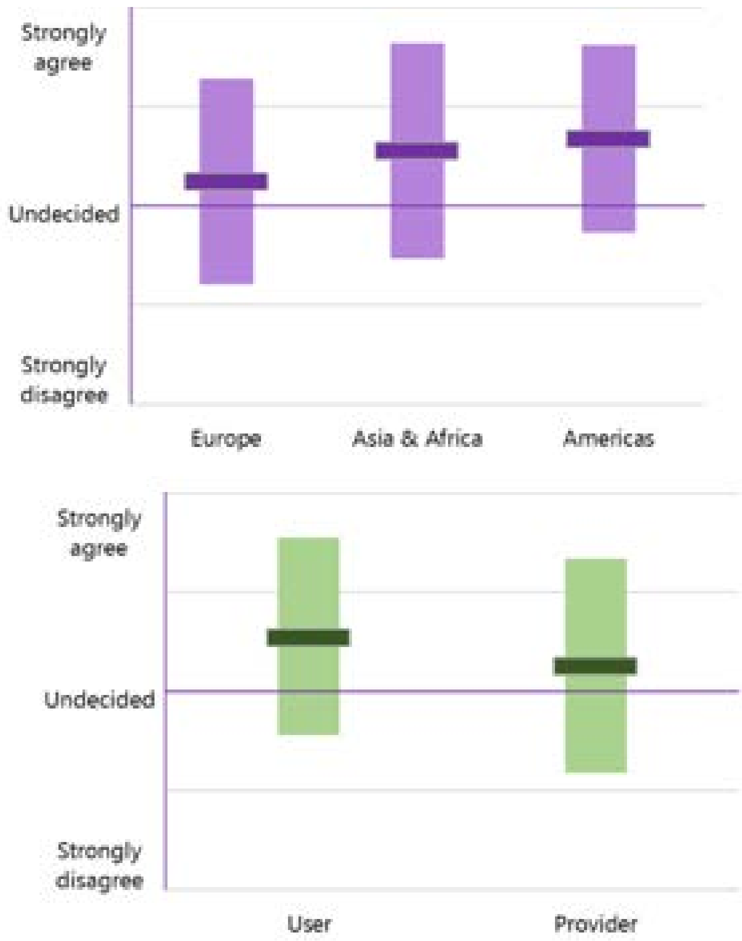
Note: The figure depicts the answers to the question by distinguishing respondents according to their geographical location and whether their institution is a user or provider of correspondent banking services. The horizontal line indicates the average response, the vertical bar indicates the standard deviation,

Figure A32.8: There is a lack of visibility of transaction related costs, i.e. who has paid which fees to whom for validation of AML/CTF, counterparty risk, liquidity reporting and credit limit.



Note: The figure depicts the answers to the question by distinguishing respondents according to their geographical location and whether their institution is a user or provider of correspondent banking services. The horizontal line indicates the average response, the vertical bar indicates the standard deviation,

Figure A32.9: Do you believe that Blockchain/Distributed Ledger Technology could be deployed as deployed as the basis for a new generation cross-border payment network?



Note: The figure depicts the answers to the question by distinguishing respondents according to their geographical location and whether their institution is a user or provider of correspondent banking services. The horizontal line indicates the average response, the vertical bar indicates the standard deviation.

Annex 3.3: CONTRIBUTORS

[redacted]

[redacted]

Chapter 4

The Future of Digital Retail Payments in Europe: A Role for a Digital Euro?

Disclaimer: This Chapter is sole authored. An earlier version has been published by and presented at a digital payment conference of the European Central Bank (see: https://www.ecb.europa.eu/pub/conferences/shared/pdf/20171130_ECB_BdI_conference/payments_conference_2017_academic_paper_wandhoefer.pdf) and has been cited in a research paper of the Norwegian Central Bank (see: https://static.norges-bank.no/contentassets/166efadb3d73419c8c50f9471be26402/nbpapers-1-2018-centralbankdigitalcurrencies.pdf?v=05/18/2018121950&ft=.pdf)

4.1 INTRODUCTION

In the context of the rapid technological and regulatory change in the field of retail payments Chapter 4 will examine this particular area in more detail. Technological change in payments is not new. In the 1990s, the arrival of e-money promised to deliver benefits of speed, transparency and efficiency to payment users. Central banks at the time questioned whether commercial bank issued e-money could create distortionary effects on monetary policy (Al-Laham et al, 2009) and thus whether they should consider issuing e-money or leave this entirely to commercial entities (BIS, 1996).

Eventually in Europe a framework for the regulation of e-money issuance was developed and e-money institutions were created.

Over the last decade the European payments market has undergone major infrastructure harmonisation with the rollout of the Single Euro Payments Area (SEPA) as well as the next wave of change with SEPA Instant Credit Transfers, launched in November 2017. The role of payment services and instruments has become a key focus for the industry, regulators and payment users, particularly given the growing levels of digitisation of services. Emerging business models of both bank and non-bank Payment Service Providers (PSPs), plus the demands of the growing e-commerce environment, are complemented by evolving regulatory requirements such as the Payment Services Directive (PSD2). With these major changes unfolding, the role of physical cash (banknotes and coins) is likely to become less relevant over time.

In addition to the European retail payment specificities, the arrival - at a global level - of private cryptocurrencies such as bitcoin, ether, dash coins and thousands of others has opened up a new chapter for the world of money and payments. These cryptocurrencies are a special form of private digital money that operates on a distributed ledger, where encryption technologies are used to manage the generation of units as well as their verification and transfer. The underlying systems are outside governments' and the banking system's control. The move from centralised to decentralised systems that achieve seamless payment transactions across the globe is hailed as a financial revolution. At the same time cryptocurrencies have the potential to challenge the role of commercial and central banks, when it comes to the provision of retail payment services.

In this broader context, one of the key the question that arises for the Eurosystem is whether physical cash will start to disappear and if so, whether the issuance of a new form of Central Bank issued Digital Fiat Currency (CBDFC) should be contemplated.

For commercial banks the subsequent question then becomes, would such a form of digital fiat compete with banks' propositions in payments and maybe beyond?

We can already observe that central banks around the world are researching and experimenting with the topic of Distributed Ledger Technology (DLT) and cryptography, where the theme of CBDFC is coming to the fore. Whilst Sweden is preparing a plan to potentially launch the 'e-Krona', the local government of Dubai has emerged as the first to launch a DLT based cryptocurrency, 'emcash', which has been declared legal tender and can be used for payments at both government related and non-governmental entities (Buck, 2017). Japan has designated bitcoins and other cryptocurrencies as payment instruments and Christine Lagarde, Head of the International Monetary Fund (IMF), has made a public statement underlining the need for governments to take cryptocurrencies more seriously as there is a risk that weaker countries may be inclined to opt for cryptocurrencies in order to reduce their dependency on the US dollar (USD) (Lagarde, 2017). Furthermore she has recently (post the publication of an earlier version of this Chapter by the European Central Bank (ECB)) underlined the importance of central banks to reconsider their role as money issuer in the digital age, emphasizing many of the key principles and design considerations discussed in this Chapter (Lagarde, 2018).

In this Chapter we will be taking a slightly different angle to the topic of CBDFC. A number of scenarios as to why the creation of a form of CBDFC would be important are outlined in the context of the broader regulatory and technology shift that the European payments market is undergoing. The Chapter continues by developing a blueprint for a new form of digital retail-use fiat currency, which preserves most of the characteristics of cash.

4.2 CONTEXTUAL BACKGROUND: THE RETAIL PAYMENTS FRAMEWORK

The following section on money, payment instrument innovation and legislation will provide the broader retail payments framework, which will form the background for the subsequent discussion of a potential CBDFC for Europe.

4.2.1 Building Blocks: Money

Let us begin with the definition of money. In classical economic theory (e.g. Jevons, 1875), money is defined by virtue of three key characteristics: medium of exchange, store of value and unit of account. It is the medium of exchange, which allows economic actors to transact with each other, i.e. it serves as a payment instrument between parties. Since the 1800s, governments have issued fiat currencies with territorial features that reflected their claim of monopoly in the issuance of banknotes. Before that time, currencies, both private and government issued, were circulating within and across borders with no territorial limitations. In a remarkable way, innovation in technology may be moving us back to an approach that is very akin to this, with the difference that currency is now digital, enabling digital commerce.

In the Eurozone, given the absence of an ECB cash office, the practical role of cash issuance and withdrawal is performed by the National Central Banks (NCBs) of the Eurozone that form together with the ECB the Eurosystem. Physical cash is the most *"visible manifestation of the central bank"* (Gray, 2006) and as highlighted by Yves Mersch (member of the ECB Executive Board), cash represents "*people's only direct link to central bank money"* (Mersch, 2017 (1)). In fact cash is the only direct claim that citizens hold against the central bank.

Mersch thus sees cash as a means to gain public support for the central bank's monetary policy and ultimately its independence. At the same time the role of cash as a store of value and means of payment fulfils a social function.

Most money today is already digital meaning that it is represented in binary form and can be moved across digital networks.

The most common form of money is 'fiat money', which has no intrinsic value. Fiat money is represented as notes, coins or digital deposits in accounts. This is different to commodity money, such as gold coins, which have an intrinsic value.

Depending on the type of money, the role of and implications for central banks differ. Two forms of money stand out: central bank issued money and commercial bank money or credit. The majority of money stock is represented by commercial bank money, while the central bank only issues a small portion, but has the task to maintain price stability for the whole stock of currency (BIS, 2003). Central bank money in the retail payment context is represented in the Eurozone by Euro banknotes, which are legal tender and constitute a non-interest-bearing liability for the ECB. All other retail payment instruments are based on electronic commercial bank money (with minor exceptions such as bank notes issued by individual banks in Scotland and Northern Ireland). A sub-category of electronic commercial bank money is e-money as defined by the European E-money Directive (2009/110/EC), which can be issued by authorised e-money institutions as well as credit institutions. E-money is fully prefunded by fiat deposits, which e-money institutions have to ring-fence with regulated credit institutions. E-money constitutes a liability for the issuing institution and European legislation requires e-money issuers to redeem e-money at par upon customer request. The amount of e-money in this specific sense in Europe is very limited.

In parallel to money that circulates within the regulated market, we have seen a growing interest in private crypto currency systems such as Bitcoin and Ethereum, which utilise cryptographic technology and are based on a distributed ledger (DL). The combination of speculation and growing popularity of Initial Coin Offerings (ICOs) as a way for FinTech companies to raise funds has led to an increase in the market valuation of these coins, where bitcoin's highs alone have reached in excess of US$101bn. of market capitalisation in 2018[27] (down to US$63.7bn. in February 2019) with more than 17.5 million bitcoins (of a maximum of 21 million) in circulation as of 16 February 2019.

Despite the emergence of thousands of cryptocurrency variants, known as 'altcoins', Bitcoin still has the largest money supply value (assuming bitcoins have a value that can be converted back to fiat currency) at 72 per cent of the major cryptocurrencies reviewed in a report by Hilemann et al. Bitcoin is followed by ether with 16 per cent and dash coins with 3 per cent (Hilemann, Rauch, 2017). More interestingly though the share of private cryptocurrency payment transactions compared with traditional fiat currency based payments is still minuscule. Most merchants and consumers still prefer to use 'real' money, and even if merchants accept bitcoins for payment, they still tend to use Cryptocurrency Exchanges to convert bitcoins into their preferred fiat currency. It is therefore still premature to ask whether central bank issued currency, or commercial bank credit, could be crowded out in the near term. Equally for a form of cryptocurrency to become a mainstream payment instrument will take time in light of significant cash usage in many European countries.

Unlike with e-money, the issuance of cryptocurrencies is not tied to a specific regulated entity and acceptance is not restricted. To make a cryptocurrency payment, there is no need for a centralised authority or

[27] See Crypto Currency Market Capitalisations for more detail: https://coinmarketcap.com/ (last accessed: 16/04/2019)

system (if the user is running an active node)[28]. The whole process takes place peer-to-peer (P2P) by using computer code, where cryptographically secured data is exchanged. This is similar to the P2P characteristic of physical cash. The process is not restricted to national boundaries or regulatory frameworks, thus allowing for an ubiquitous payment solution that can move freely within the global digital ecosystem. See Chapter 2 of this thesis for more details.

In the emerging world of private cryptocurrencies and the systems that support these, there is no clear and agreed legal regime that defines them as either a liability or asset of the respective issuing system. Many governments are analysing how to respond to this situation. For example, Japan has amended its Payment Services Act (Act No. 59 of June 24, 2009) by creating the 'Virtual Currency Law', which came into force on 1 April 2017 and recognises bitcoins and other cryptocurrencies as payment instruments. In parallel, Cryptocurrency Exchanges in Japan have to comply with know-your-customer (KYC) rules as well as liquidity and IT security requirements. These are signs that private cryptocurrencies are becoming embedded into the financial and payment ecosystem of Japan. Russia is also working on legislation that would recognise bitcoins and other cryptocurrencies as legal financial instruments and apply more rules in this space to counter money laundering. The US currently recognises bitcoins as a commodity under the Commodity Exchange Act (Shadab, 2014). Many other countries are also designing or have developed their legal and regulatory responses (e.g. Switzerland, Singapore, Dubai, the European Union etc.), but given the global nature of the phenomenon, a coherent approach would be desirable in order to mitigate potential financial stability risk, ensure consumer as well as investor protection and allow for an orderly development of this new market.

---

[28] This statement is made in the particular context of permissionless, open networks based on consensus algorithms such as PoW as used in Bitcoin (see Chapter 2).

4.2.2 Building Blocks: Payment Instruments

The last two decades have seen the payments industry in Europe together with the ECB and EU regulators pursuing a joint agenda of payment system harmonisation and service innovation, underpinned by common conduct of business legislation. The building blocks of SEPA, the PSD, as well as alignment and modernisation of Automated Clearing Houses and central bank settlement capabilities have underpinned the introduction of new euro currency-based payment instruments to the market, namely SEPA Credit Transfers, SEPA Direct Debits and SEPA Card payments.

As a further step, SEPA Instant Credit Transfers (SEPA Inst) have been launched in November 2017, delivering a cross-border instant payment solution for the euro, which provides users with a faster alternative to pay transactions up to a value of EUR 15000. The ECB is supporting this new scheme with a specially developed central bank settlement offering in the form of the TARGET Instant Payment Service, or in short TIPS. This 24/7/365 service has been launched in November 2018 and plays a key role in ensuring financial stability in this accelerated payments environment. SEPA Inst is also an enabler of new payment solutions such as ‘request to pay’, which will be able to remove frictions in the e-commerce space.

4.2.3 Building Blocks: Legislation

When looking to the regulatory drivers in European payments, PSD2 stands out as a measure that is poised to ‘change banking as we know it’. Newly introduced third-party providers (TPPs) are permitted by this legislation to access the payment account information of customers (subject to consent) that hold their accounts at Account Servicing Payment Service Providers (ASPSP), i.e. a credit institution or an e-money institution (ASPSPs can also act as TPPs). Services such as payment initiation and account information are enabled and can insert themselves into the broader digital payments economy, where Application Programming Interfaces (APIs) can be leveraged as a tool to allow account-related data transfers between ASPSPs and third parties. This opening up of payment account data unlocks the opportunity to develop new services around payments going far beyond the payment itself; e.g. data driven services will allow for automation of mortgage applications, improved credit scoring of individuals, instant consumer loans etc.

As part of the PSD2 Level 2 requirements on Secure Customer Authentication and Communication (SCA), ASPSPs will have to provide a secure communication interface, which can be an API, that TPPs can connect to in order to allow them access to the account information such that they can offer these new types of services. Creating a harmonised European API remains a challenge, however. Furthermore, payment initiation services, which today exist because of a lack of direct connection between buyers and merchants – in particular in the online e-commerce world - may become less relevant once payments execute in near real time. As soon as information about the real time execution of payments flows would directly reach these merchants, a middleman that guarantees the payments through having sight over payers’ account information may no longer be needed.

Given the open access model, all payment users will need to decide how comfortable they are with third parties accessing their payment data and what this data can or may be used for. The balance between competition – by facilitating access – and data privacy and security will be an important focus for ASPSPs and their customers, in particular in the context of the General Data Protection Regulation[29] (GDPR) (EU 2016/679) and the question of 'explicit consent', as well as data minimisation and 'the right to be forgotten'.

Another regulatory driver in European retail payments is the Card Interchange Fee Regulation (CIFR) (Regulation (EU) 2015/751), which reduced credit and debit card transaction costs for merchants. Both PSD2 and CIFR are geared towards supporting e-commerce and benefiting the merchant community.

SEPA credit transfers and direct debits also brought lower cost of cross-border payments to consumers and businesses around Europe, where pricing was kept at the level of domestic pricing with help of the Cross-border Payments Regulation (EC/924/2009).

All of these retail payment instruments and the laws that apply to them relate to commercial bank money/credit. As the market evolves towards further digitisation and as physical cash may become challenged by this, the question is whether the Eurosystem should consider issuing a digital version of what is today the only direct link it has to the citizen. To fill this research gap this Chapter develops a blueprint for a Eurosystem issued form of CBDFC, which we will label 'Digital Euro'.

[29] The GDPR is a significant European regulation, where providers are required to comply with strict personal data protection standards.

4.3 LITERATURE REVIEW

In the following we will review the growing literature on the topic of digital currency issued by a central bank and examine research on various aspects of physical cash as well as the role of privacy in retail payments. In terms of definitions, this emerging research area is characterised by the use of varying terms and meanings, reflecting the immaturity of this space. Several researchers are using the term Central Bank Digital Currency (CBDC), with some referring more specifically to Central Bank Crypto Currencies (CBCC). Others yet again refer to Virtual Currencies (VC) that can be issued by central banks. Whilst we will pick up the differing terms as deployed by various researchers in the following literature review, in this Chapter we will adopt the term Central Bank issued Digital Fiat Currency, or CBDFC, in order to underline the fact that we are talking about fiat currency as a central bank liability that comes in a new technological form. This generic term will be further defined as part of the blueprint for the Digital Euro developed in this Chapter.

4.3.1 Emerging Research on Central Bank issued forms of Digital Fiat Currency

Bech and Garratt (2017) chose to use the term CBCC for their research in this field, discussing two types of CBCC, one for the retail market and one for wholesale usage. They develop a taxonomy of money, which is based on four central properties: 1) issuance; 2) form; 3) accessibility; 4) transfer mechanism (Bech, Garratt, 2017). CBCC in that framework is defined as a currency that is: 1) central bank issued; 2) electronic and 4) peer-to-peer exchanged in a decentralised manner. Going one level deeper, two forms of CBCC are differentiated in terms of: 3) accessibility: a widely accessible retail CBCC and a restricted access wholesale application CBCC for settlement purposes. They also address the question as to whether central banks should offer a digital alternative to cash and briefly consider a cost-benefit analysis without recommending any specific solution. Papers such as the Canadian interbank settlement experiment with DLT (Project Jasper, 2017) and theoretical considerations for a potential FedCoin (Koning, 2014) can find their respective places in the new money taxonomy of Bech and Garratt.

A number of studies subsequently emerged that focus on investigating design aspects of what a broad set of researchers label CBDC and their respective implications.

For example, Bordo and Levin (2017) argue that a well-designed CBDC should be: 1) account-based. Accounts should be held directly at a central bank or made available via public-private partnerships with commercial banks; and 2) interest bearing. The CBDC interest rate could be a tool for conducting monetary policy; 3) widely available to the public and supporting the obsolescence of paper currency; 4) stable over time in terms of a broad consumer price index, which as they argue would foster true price stability. A CBDC could in their view be a costless medium of exchange, a secure store of value, and a stable unit of account.

However, they also state several potential risks including: 1) macroeconomic instability, 2) loss of monetary control, 3) systemic risks and 4) susceptibility to severe downturns. The choice of an account-based solution, as we will discuss later on, is problematic for commercial banks, which today provide this service.

Davoodalhosseini and Rivadeneyra (2018) investigate if a central bank should issue a universally accessible electronic liability. The paper examines whether new technology has changed the trade-offs between centralized and decentralized payments systems. These trade-offs depend on: 1) the technological setup, 2) improvement in the transmission of monetary policy, 3) risks to privacy and 4) impact on financial stability. They look at various proposals. Quite opposite to Bordo and Levin (2017) their main finding is that DLT and mobile computing have not significantly changed the trade-offs of providing central bank accounts to the public. They emphasize unanswered questions such as what would the quantitative impact of a central bank offered token-based system be in comparison to conventional bank deposits and bank lending?

Fung and Halaburda (2016) also investigate the question as to whether a central bank should issue digital currency and propose a framework for this. Furthermore, they suggest how to implement CBDC to improve the efficiency of the retail payment system. The three public policy questions for a central bank to consider when issuing a digital currency, according to them, are: 1) Would efficiency in payments improve? 2) Would privately issued digital currencies provide such efficiency improvements without government intervention? and 3) Is issuing a digital currency a role that a government should play? The last question is going to become more important in case private cryptocurrency circulation and usage were to significantly increase.

Building on the challenges of CBDC implications as discussed in Bordo and Levin (2017) and Davoodalhosseini and Rivadeneyra (2018), Kumhof and Noone (2018) explore the impact on the balance sheet of three models that differ in the sectors that are able to access CBDC. They suggest that if four core principles are followed, then system-wide bank runs will be unlikely, bank funding will not necessarily reduce and credit to the private sector will not contract. The principles are: 1) CBDC pays an adjustable interest rate, 2) CBDC and reserves are not convertible into fiat money, 3) no guaranteed convertibility of bank deposits into CBDC at commercial banks and 4) the central bank issues CBDC only against eligible securities.

A further perspective on monetary policy implications of CBDC is provided by Meaning et al. (2018), who explore how the monetary transmission mechanism may change under such a scenario, i.e. how a change in policy instruments (e.g. money supply or interest rates) would lead to a change in the path of the real economy. The paper argues that universally accessible, interest-bearing, account-based CBDC can be deployed as a monetary policy tool, which could enhance the monetary transmission mechanism. In particular this would allow central banks to pass on negative interest rates to the public, thus solving the Zero Lower Bound Problem (see for example McCallum, 2000).

More research on monetary policy considerations is proposed by Bjerg (2017), who evaluates three different scenarios for the implementation of CBDC: 1) CBDC co-exists with cash and commercial bank deposits, 2) CBDC co-exists only with commercial bank deposits (cash abolished) and 3) CBDC co-exists only with cash (commercial bank deposits abolished). The analysis is based on a monetary policy trilemma formulated for the domestic economy with multiple forms of money. The paper suggests that both the central bank and the commercial banking sector are money creators and that access to CBDC should be universal. The latter could in our view create unintended consequences for the commercial banking sector.

Providing a broader perspective of CBDC, a recent Committee on Payments and Market Infrastructures (CPMI) study (CPMI, 2018) analyses the potential implications this could have on payment systems, monetary policy and its transmission into the economy as well as the overall stability and structure of the financial system. Acknowledging the plethora of design options, the paper reviews the potential for a form of wholesale CBDC as well as the option of a widely available retail CBDC payment instrument. Regarding the latter the paper considers this approach of limited benefit since efficient and fast commercially provided payment products are available. In the context of the European payments landscape, as discussed in our paper, there are potential risks that could arise from commercially provided payments, which may justify a central bank provided alternative back-up solution for retail purposes. They also point to the importance of AML and raise related regulatory enforcement concerns in case of anonymous forms of CBDC. In the context of monetary policy the paper alludes to a potential expansion of the monetary policy toolkit and discusses various design related features that could create problems for the commercial banking sector, including pricing and composition of bank funding and the risk of a general flight to CBDC in times of stress.

Pieters (2017) argues that if cryptocurrencies (such as bitcoin) continue to grow, their flow size relative to international financial markets will increase. Consequently, in the context of monetary policy, central banks will need to be mindful about the fact that consumers can switch to an unregulated alternative currency.

Going deeper into the technological features of blockchain and DLT, Milne (2017) investigates the potential improvement on monetary arrangements using time-ordered immutable transaction records to record cryptocurrency transactions.

The paper argues that by putting money (government fiat money and commercial bank money) off-balance sheet, a DL can ensure the integrity of money and payment arrangements in the event of bank failure. This would mean central bank reserves would not be required for bank settlement payments and consequently there would be no requirement for 'too big to fail' protection of banks. Arguably, fully funding off balance sheet items effectively makes them on balance sheet, irrespective of the technology.

A paper with more focus on the retail payment space has been developed by Heikkinen et al (2017), who define their preferred design features of a CBDC. This new type of money should offer something beyond the existing forms of electronic money and physical cash. With technology being considered not to be a 'determining factor', a form of e-money inspired CBDC could be developed to support consumers when engaging in trade.

Practical research on a possible way forward for a digital form of fiat currency (the exact technology choice is still left open) was presented by the Swedish central bank in 2017, which discusses various methods and implications of a potential e-Krona (Riksbank, 2017 (1)). The Norwegian central bank has also recently published its first paper on the topic of CBDC, reviewing different models and potential consequences of introducing a CBDC for the Norwegian market (Olsen, 2018). An earlier draft of this Chapter has been referenced in the Norwegian paper.

With a specific view on the Eurosystem, which is also the focus of this Chapter, Lastra and Allen (2018) examine what they call 'Virtual Currencies' (VCs), differentiating privately issued from central bank issued VCs. Subject to the growth of private VCs concerns for the Eurosystem could arise in the areas of financial stability, monetary policy, AML, tax evasion and consumer protection.

Whilst the role of private VCs is still limited, they advise that the Eurosystem should act according to the precautionary principle and be prepared for future challenges in this space. Equally a pro-active and harmonised regulatory response at European level is being suggested. Both findings are consistent with the direction developed in this Chapter. A recent IMF paper (IMF, 2018) discusses different perspectives on the topic of CBDC and illuminates a series of central bank projects in this area. The paper assesses the potential for creating a CBDC across criteria that are associated to different forms of money we use today and continues by elaborating public policy goals of central banks that would need to be satisfied by a CBDC. The paper concludes that CBDC could well be the next form of money for the digital world. The use case for CBDC is considered to be primarily influenced by country specific requirements and that any plan of introducing a CBDC will need to be accompanied by appropriate design and policy considerations. The dimension of cross-border implications of a CBDC are left for future research.

And finally the BIS (BIS, 2019) published its latest survey results on CBDC covering 63 central banks. The findings of this survey indicate that central banks are cautiously approaching the topic of CBDC whilst at the same time collaborating with each other. Furthermore, the reduction of cash usage and the consequential increase of efficiency, as well as payment safety and financial stability are identified as key drivers for CBDC initiatives in the developed world, whereas financial inclusion and efficiency are more significant priorities for emerging market economies.

In conclusion, the most broadly discussed areas with regard to CBDC focus on monetary policy related aspects. None of the extant research elaborates further on the connection between physical cash, payment innovation and digitisation nor provides an in-depth proposition of a CBDFC for retail-use as a digital complement to physical cash. This Chapter aims to fill some of these gaps by proposing the rationale and blueprint for a Eurosystem issued Digital Euro that can function as a near substitute of physical cash.

4.3.2 Cash usage and cost of cash

Regarding the potential features of a new form of CBDFC, we will also lean on research done on the topic of cash.

Even though we have entered the digital payments world, cash is still the most prominent form of payment instrument in the European retail space. According to research by the ECB (Esselink, Hernandez, 2017) the usage of cash at Point of Sale (PoS) varies significantly across Europe with a share of below 54 per cent in Finland, Estonia and the Netherlands compared to above 80 per cent in Germany, Austria, Slovenia and countries in the South of Europe. According to the ECB the demand for physical cash is growing faster than nominal GDP (Mersch, 2017 (1)).

A 2016 Cash Use Index joint study of PYMTS.com and Cardtronics covering 15 Western European Countries [30] found a 0.3 per cent compound annual rate of increase of total cash use, based on a weighted average for the timeframe of 2010 to 2015, where 2.1 trillion euro of total amount of cash was used for payments in 2015. For the future, between 2015 and 2020, their report estimates a 0.7 per cent compound annual rate increase, again based on a weighted average (PAYMTS.com, Cardtronics, 2016).

By way of highlighting the degree of differences in cash usage between countries in Europe, Germany runs on a cash usage level of more than 80 per cent of transactions by volume and rising (Schmidt, 2016), whereas in Finland cash payments in retail stores were at 13 per cent in 2016 (Untiset, 2016) and in Sweden the proportion of retail cash payments has fallen from 40 per cent in 2010 to 15 per cent in 2016 (Riksbank, 2017).

---

[30] Austria, Belgium, Finland, France, Germany, Ireland, Italy, Luxembourg, Malta, Netherlands, Portugal, Spain, Sweden, Switzerland and the UK

Denmark is also an example of a country where cash makes up a mere 15 per cent of retail payment transactions at PoS, representing less than 3.5 per cent of GDP (Jensen, 2017).

Cost is another relevant aspect in the context of retail payments. Various studies have been undertaken in recent years to examine the cost of retail payments in Europe and beyond. Schmiedel, Kostova and Ruttenberg (2012) find that the cost of cash across a sample of 13 European countries, measured as the resource cost that has to be borne by all stakeholders ranging from consumers, retailers, banks, central banks, cash transportation companies, businesses etc., amounts to roughly 1 per cent of national GDP. In particular, the portion of social costs (e.g. tax evasion, counterfeit, theft etc.) associated with cash was the largest at approximately 50 per cent of the total cost identified in this study. The EC's 'Merchant Indifference Test' of 2015 represents another study, where *"for the merchants surveyed the total cost of cash represented 1.26 per cent of the total turnover"* whereas for debit cards it amounted to 0.67 per cent and for credit cards 1.17 per cent (EC, 2015).

Looking at the cost of cash from a central bank's perspective, Van Hove (2015) modelled the challenges of central bank related banknote printing costs in the context of societies that experience a steady reduction in the use of cash. His conclusion is that central banks that have decided to issue the more costly and more durable polymer notes, but are faced with a decline in demand for physical cash, should switch to reinjection of redundant notes in order to limit costs. Furthermore, he recommends that central banks relax their recall approach to old-technology based notes to allow for a longer life span of notes in a reduced cash note demand scenario, which may result in different forms of notes circulating in parallel (this may not be welcome for high denomination notes, which thus could be recalled more specifically).

None of these studies specifically examine the factor of cost of fraud or cost of counterfeit instruments, which means that the picture remains incomplete.

For example, according to the European Automated Teller Machine (ATM) Crime Report, ATM related losses due to physical attacks continue to increase, representing 27 million euro in the first six months of 2016 (European Association for Secure Transactions, 2016).

As more data becomes available, an EU-wide analysis of the economic costs of retail payments in the post-SEPA and post-card interchange regulatory context would be interesting future research.

4.3.3 Retail payments and privacy

The question of privacy is little discussed in current research on retail payments. As stated by Kahn (2018): *"When central banks first took on the job of note issuance they became privacy providers."* Privacy is becoming an increasingly important factor in a world where big data, social media and personal profiling are creating and leveraging massive amounts of data about individuals, which can easily be used to monitor, influence and even manipulate individuals and lead to identity theft. As Kahn points out, *"Not all of the privacy provided by cash is for illegal or insidious purposes, and if cash disappears we will need new ways of providing that privacy."* See also Kahn et al (2005) and McAndrews (2017) for a discussion of legitimate reasons for anonymity in payment transactions as well as Kahn and Roberds (2009) in the context of identity versus anonymity in payment transactions.

The arrival of decentralised systems and private cryptocurrencies, allowing for pseudonymity, can in part be seen as a response to the increasing lack of privacy or anonymity in non-cash payment instruments (notwithstanding the fact that most cryptocurrencies are far more transparent than conventional electronic payments).

This may also explain why cash usage for retail payments, at least in some European countries, is not decreasing but increasing. At the same time, financial stability reasons have led users to switch to private cryptocurrencies, following the financial crisis.

The IMF Staff Discussion Note on CBDC (IMF, 2018), discussed above, specifically highlights that privacy is a key user requirement and a human right (see Declaration of Human Rights).

Whereas Kahn believes that a new form of central bank issued 'e-cash' will not be able to deliver all privacy related benefits of cash (Kahn, 2018), in this Chapter we propose that a form of CBDFC, that would preserve the privacy related characteristics of cash to a large extent, should nevertheless be investigated.

4.4 RESEARCH QUESTIONS AND METHOD

In light of retail payment innovation and with a view to financial stability, data security and privacy, as well as the potential longer-term impact of private cryptocurrencies for central banks, the research questions posed in this Chapter are as follows:

"To what extent is there a rationale for the Eurosystem to develop a Digital Euro as a near substitute to physical cash? And what would be the design criteria and considerations for such a new form of digital fiat money?"

In the following we will develop the rationale and drivers for a Digital Euro and propose a theoretical framework and blueprint for the creation of this new form of central bank money.

4.5 A CBDFC RETAIL PAYMENT INSTRUMENT FOR EUROPE: WHY?

This section will discuss the potential drivers for developing a CBDFC with a key emphasis on the European payments context. We already have empirical evidence of central banks around the world experimenting with blockchains and DLT, which will help frame the discussion.

Central bank research has thus far focused on various aspects of digital currency ranging from resilience, reliability, scalability and performance to settlement finality, privacy and ease of integration with existing systems. Del Rio (2018) provides a broad overview of these activities and more recently the BIS published the findings of their survey of 63 central banks on the topic of CBDC (BIS, 2019). The BIS survey makes a distinction between wholesale CBDC and general purpose CBDC, where the latter is akin to the proposed concept of retail CBDFC proposed in this Chapter. It is worth pointing out here a few particular examples of central bank research in these two areas (Table 4.1 and 4.2), in order to set the scene.

Project	**Focus Areas**	**Status/Conclusions**
Canada Project Jasper	Interbank high value payment space: Focus on DLT system ability to meet international standards for Systemically Important Payment Systems and collaboration with the private sector. Built on Ethereum Proof of Work (PoW) system.	The work done to date has shown that the test system could meet the international standards concerning collateral, credit risk, money settlement and liquidity risk. Future research could focus on enabling pledging of general collateral, beyond cash, at the Bank of Canada. The aspect of national and/ or international integration

		with other DLT types is another area to explore.
Singapore Project Ubin	Interbank high value payments space: Development and tokenisation of a digital SGD that is used on the DL platform; a form of continuous depository receipt with no impact on monetary policy.	Phase 1 of the project focused on leveraging an Ethereum based private DL network, where Quorum was used as a consensus mechanism. A working interbank payment type was successfully developed and integration with the existing RTGS system MEPS+ was delivered. Open questions: deterministic finality, privacy, scalability, ease of integration, resiliency, Phase 2 of the project focussed on cross-border payments and DvP in the securities space.
UK	The Bank of England (BoE) has completed various DLT PoCs covering the areas of RTGS system, cross-border payments and security aspects of DLT.	The BoE continues to learn how the technology behaves as well as to identify issues and questions across the regulatory and economic spectrum.
South Africa	DLT based PoC for wholesale payment system	PoC proved faster speed and confidentiality of transactions delivered with settlement finality, resilience, scalability and regulatory oversight access. Challenges of implementation, regulatory/legal and economic factors remain.
ECB & Bank of Japan (BoJ) Project Stella	Testing the viability and characteristics of DLT based structures in the context of the ECB's RTGS service to understand if performance needs can be met. Key focus performance of liquidity savings mechanism.	Leveraging Hyperledger Fabric 0.6.1 the central banks established good results on resilience and reliability in the context of validating node failures and incorrect data format handling; good smart contract performance on the latter. The role and importance of the certification authority within the structure could however become a single point of failure risk. Trade-off between network size and

		performance was again validated. More scope for future studies around cost efficiency, oversight and market integration.
Thailand	Digital currency for interbank settlement PoC	Objective to achieve faster, cheaper transaction and validation with less intermediaries

Table 4.1 Settlement Systems Wholesale CBDC Focus

Country	**Project/Approach**	**Status/Conclusions/Next Steps**
Sweden Project E-Krona	With only 15 per cent of payment transactions made in cash in 2016 in the retail sector, Sweden seriously considers the development of the e-Krona. Focus is on consumer/retail payment, where e-Krona would be a complementary instrument next to physical cash.	Project Plan phase 1 launched in 2017. Development of theoretical proposal and system outline in progress. Phase 2 will focus on regulation and operational proposal and technologies. In 2019 we expect the decision to issue or not.
Dubai	emCash: blockchain based government issued cryptocurrency launched in October 2017	Near-Field-Communication (NFC) -enabled wallet based payments facilitating faster and lower cost retail payment transactions.
Marshall Islands	Development of Sovereign (SOV) digital currency	SOV will be introduced in 2019 as an official currency accepted alongside the U.S. dollar. The SOV is legally underpinned by the Sovereign Currency Act of 2018. The SOV will come in the form of a physical card that operates with a blockchain-enabled microprocessor, allowing users to transact in real time with zero fees and without the need for an internet connection.
China	Development of CBDC to complement fiat currency	The Digital Currency Research Lab at the People's Bank of China has filed more than 40 patent applications so far – all as part of its aim to create a digital currency combining the core features of cryptocurrency and the existing monetary system.

Uruguay	Pilot programme for e-Peso launched in November 2017	P2P digital money solution (not based on DLT), which allows exchange of e-Pesos via mobile text messages and the e-Peso app. Unique digital notes were issued to an 'e-note manager' platform for distribution, which also acted as a central register of ownership. A part of the e-Pesos issued were distributed by a third-party PSP. The pilot closed in April 2018 and next steps are being evaluated.

Table 4.2 Domestic General Purpose CBDC Focus

As reflected in the above selection of initiatives, some central banks focus more on the technical side of DLT with a view to understanding the properties of the technology in relation to the speed of interbank settlement and resiliency. Other central banks are looking at the potential of issuing their own domestic digital or cryptocurrency for economic efficiency reasons (see also BIS, 2019). Geopolitical considerations may also play a role.

The following section will elaborate a more granular rationale as to why the Eurosystem should be considering experimenting with the creation of retail-use CBDFC.

4.5.1 The Rationale for an ECB issued retail-use Digital Euro

At a general level there are several reasons as to why a central bank should investigate the topic of CBDFC. Key motivations cover the areas of monetary policy, e.g. the ability of imposing negative interest rates and improving the monetary policy transmission mechanism; currency competition (in this instance with private cryptocurrencies); efficiency of central banks' currency function; reduction of costly physical cash; payment system efficiency; security and back-up system provision; provision of legal tender once physical cash is phased out - to name a few. Many of these have been discussed in extant literature as captured by the literature review.

Below, we will develop the rationale for a particular form of digital money – a Eurosystem issued retail-use CBDFC - and discuss the needs and objectives of both the user side and the central bank. In order to guide this discussion we develop three scenarios that could emerge as the Eurozone transforms into an increasingly 'cashless society'. Our main focus is on the areas of privacy, payment security and financial stability, complemented by the political dimension around the future role of central banks as currency providers to the general public.

<u>Scenario 1: Privacy</u>

With the growth of electronic payment instrument availability and adoption, driven by the combination of PSD2, Open Banking and SEPA Instant Credit Transfers, the privacy aspects of payments will start to vanish as physical cash disappears. As a consequence consumers may demand electronic payment solutions that maintain the privacy qualities of physical cash.

Central banks prefer transparency in order to support AML/CTF regulatory compliance as well as fighting tax evasion. A middle ground will have to be found, balancing the AML/CTF and tax evasion related risks with the legitimate demand for individuals' privacy.

Scenario 2: Payment Security

As customer payment account data starts to be more exposed to different providers outside the customer's own bank/PSP (through PSD2/Open Banking etc.), this could lead to an increased risk of data related incidents. The challenge of safely protecting customer data could become more significant with data hacks and theft on the rise. In light of the requirements of GDPR in Europe and with the arrival of IoT and the embedding of payments in the digital value chain for increased automation, we could see additional risks for the security of payment and identity related information emerging, as today no controls are built into these processes. New types of questions around liability will start to arise as robots are added to the universe of payment service users. As a result, consumers may demand safer digital payment instruments from governments, rather than the private sector.

Scenario 3: Financial Stability

The increasing risks around cyber security and technical availability are another area that may warrant a central bank provided back-up solution for electronic retail payment systems. Large scale Distributed Denial of Service Attacks (DDOS) could for example take out banks' online and mobile banking services or malware could lead to ATM fraud (such as Carbanak), resulting in the unavailability of payment services. The recently experienced Visa outage (June 2018) shows how detrimental payment related system failures can be for customers.

At the same time central banks are also cognizant of the increasing cyber security challenge and the need to protect payment systems and associated data. An FMI can be viewed as a single point of failure if it uses exactly the same software in all data centres. Data security solutions such as advanced cryptography as well as decentralised processing could become relevant methods to counter the risk of attack on FMIs.

For financial stability reasons a central bank provided digital back-up solution to commercial retail payments – thus delivering a risk-free digital payment instrument (notwithstanding the overall risks of currency devaluation and inflation), a store of value and medium of exchange - would therefore be a logical next step.

Beyond these scenarios the continued existence of a central bank issued form of money for society beyond physical cash would allow the Eurosystem to maintain its direct link with European citizens. This would support strengthening the public's support of the ECB's monetary policy and thus its independence - anchored in Article 130 of the Treaty of the European Union – where the latter is instrumental in the pursuit of the ECB's central objective of price stability.

Furthermore, as reflected in the empirical research of the BIS (BIS, 2019) efficiency is another criteria for central banks in the developed world to issue a general-purpose CBDC – ranked as 'important' (3 out of 4). The particular driver here is the motivation to either respond to the reduction of physical cash in the economy or to encourage the use of electronic alternative means of payment.

4.6 BLUEPRINT FOR A EUROSYSTEM ISSUED RETAIL-USE CBDFC

At a high level, the ECB has already been conducting thought experiments in the area of digital central bank money. For example ECB Executive Board member Yves Mersch brought up the concept of 'Digital Base Money' (DBM) (Mersch, 2017 (2)). Even though DBM already exists in the form of commercial bank and other institutions' deposits held at the central bank, Mersch discusses the option to expand this to non-monetary counterparts, including citizens. A key distinction is made between a 'value-based' and an 'account based' form of DBM, where the first would have properties similar to physical cash, while in the latter case, the central bank would have to open DBM accounts for every user. The latter has also been referred to in literature as 'deposited currency account' (Tobin, 1987).

Extending the approach discussed by Mersch, this Chapter will analyse a more detailed set of questions and criteria for a Eurosystem issued DBM. Given the historical background of a general absence in the market of 'account based' central bank deposit offerings for the broader public – even though this would have been an option irrespective of digitisation - the assumption here is that the ECB is unlikely to be willing to provide account-based services to consumers, given that this is neither part of its mandate, nor is it something that would be easy to deliver without relevant experience and scale.

Our proposal builds on the value-based model and combines this with the deployment of DLT. I will refer to the new instrument as the 'Digital Euro'.

The blueprint for the Digital Euro will be developed according to the following design criteria[31] :

I. Macro Criteria	II. Legal/Regulatory Criteria	III. System Criteria
Issuance and Monetary Policy	Legal Status and Settlement	System Requirements
Financial Stability	Consumer Protection/Financial Education	Security and Resilience
Payment System Stability	Privacy and AML/CTF	

Table 4.3: Design Criteria

4.6.1 Macro criteria for a Digital Euro

In the following section we will discuss the issuance process and features of a Digital Euro and relate these to the established macro criteria.

4.6.1.1 Issuance and monetary policy

We propose that the Digital Euro would be a digital form of fiat currency issued by the Eurosystem, denominated in Euro, made available to the general public 24 hours, 7 days a week, 365 days a year in real, or near real time. Similar to physical cash, the Digital Euro would become a liability of the issuing central bank, i.e. the Eurosystem. The instrument would be for online usage only and digital wallets would store the units of the Digital Euro on each person's smart phone or other digital device. The key characteristics of cash – central bank issued,

[31] Based on the author's extensive experience in the field of payments

universal, allowing for peer-o-peer transactions and legal tender status – would be preserved.

The Eurosystem's role would be to maintain the underlying technical system, ensure issuance of Digital Euro on demand, organise transaction verification, allow for redemption and also have the ability to destroy Digital Euros. As the Digital Euro would be as far as possible the digital mirror of cash, the proposal would be to issue Digital Euros one-to-one against physical cash or electronic commercial bank balances, and leave distribution to the commercial banking system, similar to the way physical distribution of notes and coins takes place today. This method of issuance would resemble the e-money model, with the crucial difference that the type of money issued in exchange of physical cash or customers' electronic deposits held at commercial banks, would be central bank money. The size of the central bank balance sheet would remain the same given the one-for-one exchange from banknotes or electronic bank balances to Digital Euro. A similar scenario has been referred to by the Swedish Central bank for the potential issuance of an e-Krona (Riksbank, 2017).

Issuance step-by-step

Whether a customer holds an account or not, she/he could place cash at a bank, which then performs relevant KYC and AML checks and confirms receipt of cash to the relevant Eurosystem NCB, against which Digital Euro would be issued. The option of using DLT and cryptography should be investigated for purposes of mitigating risks that can arise in centralized structures, such as the Single Point of Failure Risk. Issuance of Digital Euro would technically result in the distribution of public and private cryptographic key pairs, representing the converted amounts. The same process of issuance could apply to customers that want to convert parts of their commercial bank balances to Digital Euro. To avoid dependencies on physical bank branches, ATMs could play a role for issuance in case of existing bank customers, where KYC is already in place. This could be executed in a similar way to how Bitcoin ATMs operate today. An assessment of existing and emerging consensus algorithms and surrounding technologies, such as zero knowledge proof, should be performed in line with the objectives, including privacy but also the ability to trace/identify where required for AML/CTF purposes, efficiency, speed and resilience/tamper resistance (see also Chapter 2 and the Conclusion).

In line with physical cash there would be no remuneration of Digital Euros. As Yves Mersch points out, there could be implications of negative central bank rates on banks that may therefore want to convert reserves into the new digital or crypto cash (at 0 per cent interest rate) via non-bank subsidiaries (Mersch, 2017(2)). As the Digital Euro would be limited to retail payments, this risk would not arise. Furthermore, appropriate regulations including macro-prudential policy frameworks combined with supervisory controls that leverage increased transparency and data could prevent such a risk.

4.6.1.2 Financial stability

Operating the Digital Euro on a Eurosystem-run DL would mean that traditional intermediaries in payments, primarily banks, would be able to play a role in providing services to enable distribution and redemption, as they do today for physical cash. Risks for the banking system could arise if consumers and businesses were to convert significant parts or all of their commercial bank deposits into Digital Euros, in which case banks would see their traditional customer deposit-based funding shrink. To ensure the same amount of lending activity, banks would have to replace this low-cost funding with more expensive funding available in the market. This could have negative effects on the broader economy. At the same time Jensen (2017) argues that CBDC would make commercial bank runs easier and create systemic risk, removing protection that the inefficiency of physical cash represents, i.e. ATMs will eventually be empty but the central bank would not run out of money. This could translate into a bailout of the banking system, which is not envisaged by EU legislation such as the Bank Recovery & Resolution Directive (2014/59/EU). Therefore it is crucial that our CBDFC model ensures that the substitution of commercial bank money with central bank money is limited. The proposal is to impose conversion limits. In that way, rather than destabilising the banking system the Digital Euro would be able to provide enhanced stability for the overall payment ecosystem.

Furthermore, the existence of deposit insurance regulations in Europe would help to mitigate bank run risks.

4.6.1.3 Payment system stability

As risks around cybersecurity increase – see scenario 3 - the ability of providing a back-up solution for commercially provided retail payments would be another role for the Digital Euro, which today is fulfilled by physical cash.

The features of DLT can be leveraged in order to support system resilience and reduce Single Point of Failure risks, traditionally associated with centralised systems.

4.6.2 Legal/Regulatory criteria

In addition to basic questions around legal status, there would be several elements of legislation – that today apply primarily to the commercial banking sector – which may in parts need to also apply to the Eurosystem and any entities that it may choose to outsource service provisions to.

4.6.2.1 Legal status and settlement

A decision would need to be made as to whether the Digital Euro should gain the status of legal tender, which today is anchored in Article 128 of the Treaty on the Functioning of the European Union and further underpinned by the European Commission's Guiding Principles issued as part of a Recommendation in 2010. Legal tender acceptance is mandatory at full face value, enables discharge of debt and no surcharges should apply. Declaring Digital Euro as legal tender would thus mean that, unlike in case of physical cash, technological readiness of payees becomes an important element.

A change of ownership of Digital Euro would be reflected in the exchange of cryptographic keys supported by algorithmic consensus. The legal framework of the Settlement Finality Directive (98/26/EC) may not directly be applicable to Digital Euro. However, as discussed in Chapter 2, functional settlement can occur in distributed systems by virtue of the underlying code.

To supplement this process, rules that establish legal certainty and protection for Digital Euro transactions should be developed (see also Olsen, 2018). This could for example be achieved by establishing specific provisions for settlement finality in distributed systems as an additional provision of the European Settlement Finality Directive.

4.6.2.2 Consumer protection

Regulatory measures to protect consumers would become important, as practically the loss of private cryptographic keys to access Digital Euro would be commensurate with the physical loss of cash. The Eurosystem would need to play a role in terms of supporting appropriate financial education measures and a phasing-in approach would be helpful to facilitate stakeholder readiness. An alternative avenue could be to offer forms of custodial services for cryptographic keys, akin to those available today in the private cryptocurrency space. Parts of the banking industry are currently working on developing custody solutions for any form of digital asset, which could support consumer protection in this regard.

Even though the plethora of conduct of business rules for PSPs as defined by the PSD2 in Europe would practically be difficult to apply to Digital Euro, rules around charging and pricing of Digital Euro transactions will be important. Setting policy to limit transaction fees and or prohibit surcharging by merchants in the same way as for existing electronic payment instruments (e.g. PSD2, SEPA Regulation, and EC/924/2009) would ensure a level playing field and help make the Digital Euro competitive with certain types of private cryptocurrencies.

Giving consumers more choice in payments will also become increasingly important as data analytics and artificial intelligence will allow banks and FinTechs to further monetise customer data.

Data privacy and the option for consumers to monetise their data themselves will have to be considered.

With regard to financial inclusion a central bank's core product of cash in a digitised medium would certainly help improve the market. Future research should examine this area in more detail.

4.6.2.3 Privacy and AML/CTF

Physical cash transactions, as long as below regulatory thresholds determined by governments are private. The feature of anonymity does not automatically mean that transactions made in such a way are illegitimate (Mersch, 2017 (1); Kahn et al, 2005; McAndrews, 2017). Privacy is likely going to become more important in an increasingly digitised and data transparent world that bears the risk of data and identity theft, as per scenarios 1 and 2.

A suggestion could therefore be that the Digital Euro is designed such that users are identified at the point of conversion, see issuance process described above, but that there is no linkage between identity information and the cryptographic keys used for transaction purposes. This could further be enshrined in data protection legislation, such as the GDPR. Z-cash, a private cryptocurrency that enables user anonymity, is an example of how privacy can be ensured at transactional level. In order to ascertain that existing regulatory frameworks around AML and CTF are upheld, individual transaction limits of EUR 150 in line with the fifth Anti-Money-Laundering Directive (AMLD) (EU 2018/83) could be imposed via smart contracts embedded in the core algorithm of the distributed ledger. Note here that the first progress report on the Swedish e-Krona project also suggests the option of privacy for value-based e-Krona transactions (Riksbank, 2017 (2)).

The alternative of establishing transparency on who owns which Digital Euro coin at any point in time would be unlikely to gain adoption and presupposes a high degree of citizens' trust in the central bank. Whereas this may for example reflect the situation of Denmark, where transparency and openness is a societal trait (e.g. tax returns and salaries of citizens are published on the Internet) (Jensen, 2017), it should not be forgotten that cash is a form of civil protection against surveillance and control of the population, which could become more relevant as the data economy unfolds as per scenarios 1 and 2.

4.6.4 System criteria

A multitude of considerations will need to be made in the context of a potential project to develop the Digital Euro. The Bank of International Settlements Committee on Payment Market Infrastructures' (CPMI) paper on 'Distributed ledger technology in payment, clearing and settlement' (BIS, 2017) provides a good first pass at relevant questions that will need to be asked in the broader context of DLT. IMF research has also focused on a number of questions that will arise in terms of user and central bank requirements in the context of digital fiat currency (IMF, 2018).

4.6.4.1 System requirements

Key criteria for the Eurosystem would encompass technology safety and efficiency as well as cyber resilience and overall system agility. The choice of DLT would need to be carefully considered and tested, but the proposal here is that the deployment of a private permissioned ledger structure with the option of enabling third party node verification that could be provided by the participating Eurosystem central banks – reflecting the already distributed nature of the Eurosystem in a DLT structure – would be a potentially well suited technical model for the Digital Euro.

As discussed above, by virtue of distributing the system for the Digital Euro across the Eurosystem's NCBs resiliency could be enhanced through removal of risks such as the Single Point of Failure Risk. The risk of double spending Digital Euro would be tackled as part of the consensus mechanism of the DL.

The choice of consensus protocol would determine how efficient and speedy the transaction verification and execution would be. The Monetary Authority of Singapore (MAS) has experimented with different permissioned DLT solutions including the deployment of the Quorum consensus algorithm that enables Raft Consensus[32], which allows for privacy and has significant advantages for the regulated industry compared to permissionless structures that use for example PoW (such as in Bitcoin). The many emerging consensus algorithms, referred to briefly in Chapter 2, will need to be further researched and experimented with. As more efficient forms of DLs and consensus algorithms, compared to the Bitcoin PoW blockchain, are beginning to emerge, the Bitcoin related criticisms raised by BIS and others, will become less relevant (BIS, 2018).

The problems associated with physical cash such as security risks in physical cash transports or ATM related security concerns would become much less of a problem. Different forms of technology and data related security risks may however arise and would need to be identified and managed. More research would have to be undertaken in this space in order to balance efficiency, resilience, privacy and security.

4.6.4.2 Security and resilience

The Eurosystem as the issuing institution would be responsible for the overall Digital Euro framework, i.e. maintain the DL and ensure a resilient operating model. Digital wallet solutions would likely be provided by third parties that have the required expertise and

[32] The RAFT Algorithm has been developed by Diego Ongaro and John Ousterhout of Stanford University with the purpose of increasing understandability in order to enable easier implementation compared to Paxos algorithms.

technology. Appropriate security policies and standards would need to be developed by the Eurosystem to ensure safety of wallet solutions. The role of commercial banks as distribution channels for Digital Euros would also need to be clearly defined as part of the appropriate policy framework. Custodial services could be provided by the banking industry in terms of further supporting resilience and protection of consumers.

4.7 RESULTS AND DISCUSSION

This Chapter adds to the growing literature on CBDC by developing a unique perspective for a retail payment CBDFC. Since an earlier version of this Chapter was presented to and published by the European Central Bank[33] more literature has been developed on the topic of CBDC discussing the opportunities, challenges and implications of such a form of money across monetary policy, financial stability and efficiency as well as proposing various design considerations. This Chapter develops the argument for a CBDFC retail Digital Euro as both a financial stability enhancing measure and as a tool to maintain citizen's privacy and security in low value payments, in response to the many regulatory and digital challenges that will unfold across the European payment landscape in the coming years.

Issuance of a form of Digital Euro is motivated by three distinct scenarios: 1) the demand for citizen privacy in low value retail payments as physical cash becomes less available, 2) a response to citizen concerns with payment data security issues in commercial bank provided payments and 3) as a means to manage financial stability risks that can emerge in the context of cyber-attacks and operational failures.

We further develop a theoretical blueprint and set of design criteria that serve as practical guidance on how this new form of digital cash could be delivered. Table 4.4 summarises the proposal for the Digital Euro across the discussed key variables and contrasts this with other forms of money, both traditional and emerging.

---

[33] This paper was presented at the ECB's "Digital transformation of the retail payments ecosystem" conference in November 2018. See following link to conference web-site (last accessed 8/8/2018):

https://www.ecb.europa.eu/pub/conferences/html/20171130_ECB-BdI_digital_transformation_of_the_retail_payments_ecosystem.en.html

Key characteristics & processes	Fiat money (notes & coins)	Electronic commercial bank money	Bitcoin (as a specific example of a private cryptocurrency)	CBDFC (Digital Euro)
Issuance Process	Notes are printed by the central bank; the mint creates coins.	Commercial bank issued liability (credit creation). Electronically credited to a central bank reserve account.	Mining nodes on the network are awarded Bitcoins each time they find the solution to a certain mathematical problem (and thereby create a new block).	Central bank issued.
Format	physical	electronic	electronic	electronic
Money supply and mechanism of creation	The supply is controlled through issuance and redemption process.	The supply is indirectly controlled by the central bank altering interest rates on lending to banks as well as changes in fractional reserve banking rules.	The reward for solving a block (i.e. money issuance) is automatically adjusted so that every four years of operation of the Bitcoin network, half the amount of Bitcoins created in the prior four years are created. The total number of coins cannot exceed 21 million (deflationary currency). Bitcoins cannot be destroyed, but something akin to destruction results when private crypto keys are lost.	Money supply controlled by Eurosystem. Ability to exchange physical cash and electronic money 1:1 against Digital Euro, with overall limits imposed.
Claim on issuer	Yes	Yes	No	Yes
Primary Record	Central Bank (at time of issuance)	Core Banking System	Distributed Blockchain	Central Bank (at time of issuance)
Interest rate based remuneration	No	Yes, but negative interest rates could also apply	No	No
Assertion of ownership	The holder of the physical item denotes ownership.	Ownership by the account holder is validated by the authority of the bank that provides the account.	Each transacting participant in Bitcoin has control of one or more unique public/private crypto key pairs. The sequence of ownership changes of any coin is encoded into the block chain such that at any time one can read the total of coins at any one address. What is not asserted, however, is a	Proposal to create a similar model to private cryptocurrencies in terms of the public/private crypto key pairs. Consensus algorithm to be determined.

			connection between that key and the owner's true identity.	
Legal/regulatory status	Cash is legal tender in Europe; payment process itself is unregulated	Regulated deposit taking activities and payment service provision is subject to national conduct rules and consumer protection.	The specific treatment differs across geographies. Several governments apply rules to Bitcoin exchanges and levy tax on Bitcoin related gains.	Legal tender status to be determined.
Finality of payment	Through the direct transfer of bank notes from one person to another.	Transactions settle with 'ultimate finality' (i.e. final settlement in central bank money) through a movement of funds between commercial bank accounts held at the central bank.	Bitcoin achieves probabilistic settlement, which can be expressed in degree of settlement finality (DSF), which increase with the publication of subsequent blocks (h) in the chain. The DSF required for final settlement is equal to h*+6, which translates into 1 hour (see Chapter 2). Note that there is no applicable concept of legal settlement finality.	Regulatory regime to be expanded to include legal certainty of settlement finality in distributed systems. Settlement asset is central bank money.
Anonymity of transactions	Yes	No. Unique bank accounts associated with personal/legal identity are used to reflect an electronic record of transfer events, increment and decrement of balances.	Pseudonymous users; identification of actors that own cryptocurrencies, but that do not make use of Cryptocurrency Exchanges can be more complicated to trace, but it is technically possible.	Yes, but option to trace suspicious transactions in case of suspicious activity patterns.
Money laundering detection and payment screening	Money in cash form is reasonably difficult to launder in large amounts. Numbering on cash notes makes tracing possible.	A lot of resources required detecting and deterring money laundering. Data analysis tools are used to help automate this process.	Bitcoin assumes no connection between addresses and actual identities. But all movements of any "Coin" are recorded; all addresses of all senders and recipients are recorded. Those records are immutable and accessible, which makes it easier than tracing cash. Many Cryptocurrency Exchanges are now required by law to identify their users. For those that do not, this leaves opportunities to exchange fiat	Proposal as AML/CTF mitigation measure to limit any -cash transaction to EUR 150 (as per 5th EU AML Directive). AML/CTF traceability in ledger, subject to suspicion.

			currency obtained from illicit activities into crypto currency.	
Security	Notes and coins can be forged, but technology advancements are employed to reduce the risk of forgery.	Security protocols controlling who initiates electronic transfers. Identity verification, card PINs and double entry bookkeeping etc. are all used to reduce security risks.	Security risks exist in relation to crypto wallets and keeping access to private crypto keys secure. As blockchain embeds cryptography in the protocol, which differs from other digital systems, the risks are really at the edges; i.e. Cryptocurrency Exchanges and wallets.	Crypto wallets can be hacked. Risk should be mitigated by deploying security resilient wallet solutions, which should be vetted by the Eurosystem.
Handling of double spending problem	The physical nature of cash makes it impossible to double spend. It physically moves towards the intended owner.	Unique transaction IDs; software to flag duplicate payments; reconciliation systems.	The ordered time stamped and linked encrypted record of all transactions is extremely difficult to falsify. An attempt at re-spending would be mathematically rejected by all validating nodes in the system. However, if more than 50 per cent of the miners colluded, they could forcibly confirm a forked version of that history wherein a number of coins could be double spent.	Similar to Bitcoin model in terms of time stamping. A more efficient and yet secure consensus mechanism should be deployed.
Physical/Cyber Attack risk	Risk of physical attack to steal cash is high. Physical security measures, i.e. protection in vaults and transport with security vans are therefore important.	Yes; banking systems take required precautions to prevent attacks. Many types of fraud activity take place, such as identity theft, phishing, social engineering, cyber-attacks, malware etc.	The Bitcoin blockchain has never been hacked.	Digital Euro should be developed in a cyber-resilient way. The distributed nature of the ledger can help remove Single Point of Failure Risk.

Table 4.4 Digital Euro and other money types and their characteristics in the context of retail payments

4.7.1 Implications for theory

Since an earlier version of this Chapter was presented to and published by the European Central Bank more literature has been developed on the topic of CBDC discussing opportunities, challenges and implications of such a form of money across the areas of monetary policy, financial stability and efficiency as well as proposing various design considerations. This Chapter adds to the literature by developing a unique perspective for a retail payment CBDFC. Empirical evidence on different experiments with general purpose CBDC, as discussed in this Chapter, echoes the relevance of this approach.

Future theoretical and practical research will need to focus on the broader question of what role central banks should play in a future of digital money.

4.7.2 Practical implications for the broader industry and future research suggestions

A Digital Euro would deliver a technical variant of fiat money, which combines some of the characteristics of physical cash with those of e-money. The opportunity to establish transaction value limits as well as the ability to trace pseudonymous transactions for AML/CTF related reasons represents a clear advantage over physical cash. Technology can deliver P2P payment capability and the efficiency of the process is likely to facilitate merchant acceptance.

Consumer education on the features and function of the Digital Euro will be important but should be underpinned by legal protection (à la PSD) and complemented by additional services such as custody of cryptographic keys. Challenges for financial stability, monetary policy and the commercial banking industry – discussed in current literature - could be mitigated under the proposed design.

Obviously a full-scale roll out of Digital Euro could encounter a number of challenges that would need to be overcome. Whilst DLT is poised to provide a technical opportunity to improve payments across various aspects in comparison to the status quo, including resiliency, reconciliation, transaction speed and potentially cost, it is still a continuously evolving technology, which has not yet reached a state of maturity. Key criticisms today often relate to high latency, cost of processing (e.g. energy consumption of mining bitcoins) and questions around transparency. However, the proposal of creating a back-up solution on a different technology stack merits further investigation in terms of the contingency benefits that this would deliver. Furthermore, technology advances in the space of cryptography, such as attribute based randomised encryption could deliver significant improvements to data security and should be examined more closely.

Another question, which is particularly relevant in the context of retail payments, is whether cryptocurrency, even if government issued, could become a broadly used means of payment any time soon. Given the high levels of cash usage and the still very low adoption rates of private cryptocurrencies such as bitcoins for payment purposes, the latter mostly being used for buy and hold purposes (i.e. more of a 'crypto asset'), the speed of adoption of the Digital Euro would likely vary across Europe. Means of incentivising adoption including policy measures to support consumer protection would have to be contemplated.

The banking side of the market may perceive the Digital Euro as a competing payment instrument and the role of the central bank in providing a new form of central bank money for retail use would need to be clearly defined in order to maintain balanced competition in the market.

As digitisation advances and different forms of money appear, central banks will have to develop their vision for the future of money and explore the new possibilities that technology advances present in order to deliver this future.

Dr. Iris Hineman: "Sometimes, in order to see the light, you have to risk the dark."

Minority Report

Chapter 5

Conclusion

The payments world is undergoing rapid change. With the arrival of new technologies that allow taking out the middle-men, fundamental questions such as: 'Who should run the financial system and how?' and 'What is money in a digital future of connected machines?' - are beginning to arise. Literature in the space of technology innovation, financial stability and payments is limited, which is why we have set off to shed some light onto these issues.

5.1 SUMMARY AND CONCLUSIONS

This thesis is composed of three main chapters.

In Chapter 2 *(Proof-of-Work blockchains and Settlement Finality: a functional interpretation?)* we theoretically modelled the Proof-of-Work (PoW) blockchain, exemplified by Bitcoin, with a view to answering the question of whether settlement finality is achieved in this system. We deliberately chose to focus on the PoW blockchain as it has demonstrated the capability of transferring digital value between untrusted parties. At the same time we are fully cognizant of the many drawbacks that this model entails in terms of efficiency, latency, scalability and cost. By expanding the theoretical Uniform Functional Model for the financial infrastructure (UFM) we validated the applicability of this model in light of the radically innovative and different system of the PoW blockchain. Modelling PoW across two distinct scenarios, we also identified where counterparty and settlement risks occur and showed that within the closed system of the blockchain these risks have no applicability. This insight demonstrates that new technologies enable us to embed settlement finality within the system itself. As a consequence we have developed a new definition of settlement finality for PoW blockchains, to complement the broader literature on settlement finality in traditional financial systems. Finally, we assessed the features of PoW settlement in comparison to the existing legal framework for settlement finality and found that, in practical terms, system immanent settlement finality is preferable to the alternative of legal enforceability ex post. In other words, having prefunded accounts, conceptually reflecting the Bitcoin model, is different to the current FMI operating model of settlement accounts, where the latter offer several options of funding such as increasing collateral held at the central bank or raising intraday liquidity.

In case there is a lack of funds on the day of settlement, the ability to legally enforce settlement finality does not solve the problem of funds shortage and systemic risks can arise. This finding is however qualified by the caveats of the current significant shortcomings of PoW blockchains as they relate to inefficiencies and cost, high latency, scalability limitations, 51% attack risk and fork related risks of users not receiving newly created coins.

In Chapter 3 (*The Future of Correspondent Banking Cross Border Payments*), focusing on cross-border payments, we analysed and empirically validated the challenges and risks of this business and developed a set of requirements for what a future improved model of this business could look like. In line with our objectives, we further constructed a set of design scenarios for cross-border correspondent banking payments and provided a qualitative ranking of these in terms of feasibility, efficiency and overall ability to satisfy the identified requirements. These were complemented by a set of policy and governance related recommendations, primarily addressed to national and international regulators. Our conclusion shows that the SWIFT global payments innovation (gpi) implementation by financial institutions (FIs) has the potential to address financial stability and risk-related problems in the inter-bank space via transparency and real-time flows of data. Consistent with the statement that 'data is the new oil', our finding is of particular relevance to the industry as it removes the distractions associated to radical and still immature innovations such as DLT and Artificial Intelligence (AI) and instead focuses the minds on leveraging the vast amount of data we already have with the help of more mature technology solutions.

In Chapter 4, (*The Future of Digital Retail Payments in Europe: A role for a Digital Euro?)* we studied how a Digital Euro could deliver the digital version of fiat money, which would combine some of the characteristics of physical cash with those of electronic money. Our findings provided a basis for taking internal research and experimentation within the Eurosystem forward. With emerging literature and market commentary on this topic, the perspective that we are offering in this research is unique and important at the same time. Unique in the sense that the retail payment space tends to get overlooked by central banks as long as physical cash is still prominent. Important in the sense that regulatory change and innovation are leading us into an Open Banking and open data economy, where security, privacy and resilience are going to become more important and more challenged as we move forward.

5.2 IMPLICATIONS FOR INDUSTRY, REGULATORS AND CENTRAL BANKS

The aim of this thesis is to deliver applied research. Therefore, the following section will provide the many insights that we gained from this Chapter. The key stakeholders for whom our research is most relevant are the banking industry, central banks and regulators.

5.2.1 Implications for the Banking Industry

The findings of our modelling of PoW demonstrate that there are technology innovations in the DLT space that are capable of removing counterparty risk, enabling automatic reconciliation of data across all participants in a ledger and providing a digital audit trail, which is important for both business and regulatory purposes. As new forms of DLT are being designed to address the requirements of the regulated financial industry, it will be important to maintain the embedded feature of functional settlement as this provides a clear benefit to financial stability. The industry should stay involved both in terms of research and experimentation as well as gradual implementation of these types of new technologies, where practical. New forms of consensus protocols that combine immutability and functional settlement with more efficient forms of validation in the context of a closed user group of regulated entities should (and need to) be developed in order to support viable models that the regulated banking industry could adopt in future.

With regard to our research on the future of cross-border payments the first implication of our findings is that banks using SWIFT should urgently and wholeheartedly embrace and implement gpi. Working actively with the SWIFT community to make gpi a success across the network will deliver the benefit of enhanced data and transparency, which are the new methods for managing counterparty and operational risk.

gpi next generation as it is laid out today will have the power to address the settlement risks in the high value payment space and further connect banks end to end in a more transparent way. This transparency and real-time information will help re-build trust between banks and enable institutions to act early on as risks start building up. The policy recommendations of this research should be consistently communicated by banks to their regulators in order to arrive at a more globally cohesive framework for KYC, AML, CTF and conduct of business practice. Future avenues that could leverage the evolving DLT stack should be further explored and SWIFT could play a leading role in helping design solutions for the community. It is positive to note that in January 2019 SWIFT announced its plans to launch a PoC for a gateway – labelled gpi Link – that would allow blockchain connectivity to its gpi platform. These steps indicate that SWIFT is going to pursue more active steps in relation to DLT, which align with our proposals for next steps in Chapter 3.

In the context of the potential future of Central Bank Digital Fiat Currency (CBDFC), the role of the banking industry should be to continue supporting security and data privacy in the context of the evolving commercial bank retail payments offering. At the same time the commercial banking sector should support the idea of a future role for the Eurosystem in digital retail payments. Banks would need to be part of the overall framework as they are the gatekeepers to the customer, the controller of KYC. Supporting distribution and redemption of the Digital Euro would become an important function of banks. The initial stages of exploring technical, governance and regulatory aspects of the Digital Euro PoC should be taken by the Eurosystem.

5.2.2 Implications for Central Banks

The work on PoW and settlement finality is a key area for central banks in terms of understanding whether elements of DLT and associated consensus algorithms could help remove counterparty risk. In particular for central bank operated FMIs, such as RTGS systems, investigating the risks and opportunities of this emerging technology is of great importance. Whereas central bank research into DLT has been performed by some institutions, this should become a broader effort and settlement finality related aspects should be emphasized more strongly. Our proposed definition of functional settlement for PoW-type DLs expressed in the form of degrees of settlement finality (DSF) can constitute the beginning of what could become a plethora of different nuances of settlement finality models depending on the design of DLs and consensus algorithms.

In relation to cross-border payments there is a recurring question as to whether central banks should be more deeply involved in providing cross-border settlement in central bank money. A first step and implication of our research is for central banks to embrace gpi with their systems – gpi for FMIs - such that we have a transparent end-to-end flow of payments related data. Alternative models such as synchronisation and future experiments to connect RTGS systems across borders, with the help of DLs or other technologies should be explored further. Recent joint research by the Bank of Canada, the Bank of England and the Singapore MAS, which discusses the potential for a form of Wholesale Central Bank Digital Currency in combination with DLT, that could support more efficient cross-border payments (BoE, BoC, MAS, 2018) is a first step in that direction.

Our third contribution on the topic of CBDFC is a clear call for the Eurosystem and other central banks alike to explore in more practical terms the idea of CBDFC from a technological, governance and regulatory perspective. In the European context the potential risks of Open Banking, PSD2 and cyber security as well as the importance of privacy in retail payments will have to be taken seriously by the Eurosystem. Despite the growing literature in this space, most of the emphasis continues to be placed on monetary policy aspects, rather than the role of central banks in payments as well as the operational dimension of payments. It is important to connect all of these aspects as the role in payments is tightly linked to higher order concepts such as sovereignty and the expression such in fiat currency terms. As the underlying technology of money evolves, central banks should not fall behind as otherwise no one will use 'their money' in the future and this would have considerable implications on the way our societies will operate.

5.2.3 Implications for Regulators

The importance of our PoW settlement finality research is particularly relevant for regulators as this analysis demonstrates that aspects of law can now be reflected in computer code. However, there is a more fundamental challenge with blockchain and DLT more generally. The technology provides a platform for redesigning business models and processes. This redesign has the potential to change the roles and responsibilities of market participants. Rules and regulations are written based on a fundamental understanding of the role that each party plays in a particular scenario. When blockchain/DLT changes this role, new legal frameworks will need to be developed. Linear relationships (service provider and client) and obligations in those relationships (e.g. due diligence) need to be reconsidered in this new world.

The challenge for regulators is not just to adapt quickly enough to keep pace with the rapid advancement of technology, but to write rules that remain practical and applicable even as technology continues to evolve. Technology neutral language that facilitates innovation, but at the same time addresses the emerging and potential new risks will be required. This is not an easy task to undertake.

Considering cross-border payments, regulators should play a far more active role in helping to create global consistency of AML/CTF rules, encouraging implementation of the LEI into payment systems messages and supporting information sharing on suspicious transaction between FIs. At supranational level bodies such as the Financial Stability Board (FSB) and the Basel Committee could use their influence and governance processes in order to establish a best practice framework for national KYC registries and evaluate countries accordingly, re-using the peer review process that today applies in the context of Basel rule compliance.

Implications for regulators arising from our CBDFC proposal range across regulatory and practical challenges that are likely to unfold in Europe and other jurisdictions with similar approaches. The consequences of regulatory measures to drive competition by opening up customer account information to lightly regulated third parties will unfold in the coming years. With cybersecurity challenges the increased risk of private data exposure to unknown parties is an area that could swing public opinion once significant incidents start occurring. Regulators will need to be on stand-by to modify regulatory requirements where needed and to ensure the development of deeper expertise in order to be able to effectively supervise the increasingly complex PSP ecosystem. New technologies including DLT may be helpful in automating some of this supervision, supporting regulators in their role as controllers of the market place. A CBDFC as a secure back-up system for physical cash and a privacy enhancing retail solution should be on their agenda.

5.3 LIMITATIONS

First of all, our research is limited to aspects of the 'here and now'. With a rapidly evolving payments landscape, fueled by both technology advances and regulatory change, we had to choose specific areas of focus, which meant that we naturally had limitations.

Our research on settlement finality is restricted to the example of the PoW consensus model in the Bitcoin blockchain. Since the arrival of Bitcoin we have seen a lot of innovation in this space, both in terms of the creation of 1000s of new altcoins but also more fundamentally with regard to alternative consensus protocols, permissioned and semi-permissioned DLs and differing degrees of privacy of data within ledgers. Whilst our research is a first step into the settlement related aspects of DLT, more research will naturally have to be developed as systems and solutions evolve.

The ambition of our cross-border analysis is focused on providing practical recommendations for industry (both banks and technology firms), regulators and central banks/supranational bodies over the next 5 – 10 years. We cannot at this stage anticipate the speed of technology evolution and adoption, which is why we remained conservative, allowing for significant improvements without radical change requirements on stakeholders. More research on theoretical models for cross-border payments based on CBDFC (see Chapter 4) where left for future research instead.

And finally, the CBDFC blueprint for a Digital Euro has been designed with the specificities of Europe in mind, given the particular regulatory and innovation framework that is in place as well as the nature of the Eurosystem itself. Some elements of this research can be transposed into a more generic discussion on digital retail fiat currency issued by central banks.

So far we only have one live example, that of ‘emCash’ in Dubai, in addition to pilots such as the e-Peso in Uruguay and the upcoming SOV digital currency for the Marshall Islands. More experiments are likely to follow, which will provide scope to further expand our model.

5.4 FUTURE RESEARCH

It is clear that in certain situations blockchain and DLs more generally are a technology that could deliver unique benefits. However with new opportunities come new challenges and widespread adoption of blockchain is dependent on a number of these being addressed.

Future research in the context of blockchain/DLT and the role this can play in money, payments and settlement should therefore focus on the following areas.

As shown in Chapter 2, the underlying consensus algorithm of PoW in Bitcoin does fulfil the conditions for completion of functional settlement in a completely trustless environment. However, the way in which this is achieved is complex, expensive, slow and not scalable. In order for the financial industry to leverage DLT, a more efficient way of operating the ledger consensus mechanism will have to be found. Whilst we have seen the emergence of various forms of permissioned, closed-user group, blockchains that operate on much lighter consensus mechanisms, these are no longer immutable or tamper resistant. Because it has to be assumed that not all participants in a closed-user DL structure – even if these are regulated banks – are honest nodes, more research and development will have to go into delivering immutability, tamper resistance as well as efficiency, low cost, speed and scale. The Distributed Random Master Election (DRME) method for random-based non-interactive leader election in a distributed network could become a promising solution for this, in particular in combination with the use of zero-knowledge proof to ensure that data on the DL is kept secure and private, only allowing the interacting counterparties and potentially regulators to access the data.

Another area that research should focus on is to resolve the tension between the need for transparency and the desire for privacy. The transparency of the shared permissionless ledger of the Bitcoin blockchain brings with it the promise of greater integrity and accountability across an ecosystem, increased trust amongst participants and a reduction in counter-party risk. However, there are many legitimate reasons as to why parties may not want to grant full visibility to their data. Tailored transparency needs to be developed, with slices of information shared on a need-to-know basis. This issue is one that has attracted significant industry attention and activity. Solutions for this are in the process of being developed (see our discussion in Chapter 4), but it remains to be seen whether they can operate at enterprise level scale. Improved solutions in this space would also be able to cater for compliance with the EU data protection 'right to be forgotten'. Meeting data protection obligations, whilst still achieving the original objective, requires careful consideration and design.

Whilst DLT can be transformative, integration with existing systems will be required. This is not only an issue of implementation costs, there is also architectural complexity with the connectivity and integration between the old and the new systems. Such integration requires significant thought about the legal, operational, technical and commercial considerations and skilled design.

There also needs to be consideration of whether any manual steps in the process would deliver a better or even different result. For example, in a smart contract, a machine makes a decision based on available criteria according to pre-programmed logic or algorithms. The decision making process is objective. Humans, on the other hand, bring subjectivity into a decision making process, which can have its downsides (for example, bias and prejudice). However, at the same time humans are better at taking into account context, individual circumstance and all the shades of grey that exist in life.

In the area of cross-border payments our research has identified that many of the issues in this business relate to regulatory requirements and associated risks of non-compliance. Future research should therefore explore different paths of regulatory harmonisation and standardisation that would remove the current barriers of fragmentation.

Furthermore, exploring blockchain/DLT in relation to interoperability with gpi is another area of future research, which according to recent indications by SWIFT is going to progress in 2019 and beyond.

Research by the central bank community into different models for cross-border connectivity should intensify as digitisation technologies start to enable interconnectivity. In particular, regulatory and monetary policy related questions will need to be addressed, in order to realise the potential benefits that technology can bring to financial stability in this space.

As digitisation advances and different forms of money appear, central banks will have to develop their vision for the future of money and explore the new possibilities that technology advances present in order to deliver this future. The proposal of developing a new form of Central Bank Digital Fiat Currency, should be researched not only for the purpose of technology experimentation and learning but also with a focus on market structure and policy related questions.

The question of efficiency and cost in the broader context of legacy IT systems will also need to be addressed. A key reason for the slow uptake of DLT in the financial services industry is the challenge of interoperability with existing systems and the operational risks that can arise when managing across different systems and technology stacks.

An overarching question that would need to be addressed more specifically is 'Can you really have a decentralised system?' For the regulated industry the key benefit of DLT lies in the distribution, rather than the decentralisation. Distribution in this context is an operational concept, whereas decentralisation is about having a multitude of actors that set the rules by consensus. Distributing the settlement process across many computers will support operational resilience. But a decentralised approach, i.e. no central governance, in relation to the underlying system code would not be appropriate. The benefit of being able to include regulatory requirements in the base of a DL would mean that the system is centralised when it comes to rules and governance, which can be embedded in computer code. Enabling participants to change the underlying rules and thus the code could result in chaos, a risk that even the Bitcoin community is acutely aware of.

Despite all of these open questions, news of blockchain and DLT implementations around the world have become a weekly and sometimes even daily phenomenon. Whether it is commercial banks launching mobile apps for blockchain-based international payment services to retail customers fueled by blockchain FinTechs (12 April 2018), the World Bank collaborating with commercial banks to launch an Ethereum-based platform for blockchain bond issuance (11 August 2018), or the London Stock Exchange Group working with a Fintech in order to build a blockchain platform for corporate equity issuance (11 July 2018), it is all happening right now and it all will contribute to creating a more mature technology that can support the evolving digital financial ecosystem. But we need to ensure that governance, laws as well as code work together to support financial stability and security.

We are at the beginning of something big – and we are already down the rabbit hole….

REFERENCES

Al-Laham, M., Al-Tarawneh Albalqa, H., Abdallat, N., (2009), "Development of Electronic Money and Its Impact on the Central Bank Role and Monetary Policy", Issues in Informing Science and Information Technology, Volume 6, 2009, Jordan.

Alleyne, T., Bouhga-Hagbe, J., Dowling, T., Kovtun, D., Myrvoda, A., Okwuokei, J., Turunen, J., (2017) "Loss of Correspondent Banking Relationships in the Caribbean: Trends, Impact, and Policy Options", IMF Working Paper, WP/17/209.

Angelini, P. (1998) "An analysis of competitive externalities in gross settlement systems", Banking Finance 22, 1–18.

Back: Hashcash developed in Back (2002).

Bank of Canada, Bank of England, Singapore MAS, (2018) "Cross-border interbank payments and settlements – emerging opportunities for digital transformation", November 2018.

Bank for International Settlements (BIS). "Glossary", Basel. Switzerland.

Bank for International Settlements (BIS). (2003) "The role of central bank money in payment systems", Committee on Payment and Settlement Systems. Basel. Switzerland.

Bank for International Settlements, (2016), "Implications for central banks of the development of electronic money", Basel. Switzerland.

Bank for International Settlements (BIS). (2017) "Central bank cryptocurrencies", Quarterly Review. Basel. Switzerland.

Bank for International Settlements, (2018), "Annual Economic Report", Basel. Switzerland.

Bank for International Settlements, (2019), “Proceeding with caution – a survey on central bank digital currency”, BIS Paper No. 101, Basel. Switzerland.

Bank of England (2018) “RTGS Renewal Programme: Synchronisation Workshop”, London.

Baran, P., (1962) “On distributed communication network”, The Rand Corporation, Santa Monica, California.

Baregheh, A., Rowley, J., Sambrook, S., (2009) “Towards a multidisciplinary definition of innovation”, Journal of Management Decisions 47 (80), September 2009.

Barrdear, J., Kumhof, M., (2016) “The macroeconomics of central bank issued digital currencies”, Staff Working Paper No. 605, Bank of England, London.

Basel Committee on Banking Supervision, (2009), “Due diligence and transparency regarding cover payment messages related to cross-border wire transfers”, Basel, Switzerland.

Bech, M. L., Garratt, R., (2017), “Central Bank Cryptocurrencies”, BIS Quarterly Review, Bank for International Settlements, Basel, Switzerland.

Bech, M. Shimuzu, Y., Wong, P., (2017), “The quest for speed in payments”, BIS Quarterly Review, March 2017.

Berndsen, R. J., (2013), “Towards a Uniform Functional Model of the financial infrastructure”, Journal of Financial Market Infrastructure. 2(2), 77–108.

Bjerg, O., (2017),”Designing New Money - The Policy Trilemma of Central Bank Digital Currency”, Copenhagen Business School Working Paper. Denmark.

Böhme, R., Christin, N., Edelman, B., Moore, T., (2015), “Bitcoin: Economics, Technology and Governance”, Journal of Economic Perspectives, Vol.29, No.2 (Spring 2015), 213-238.

Bordo, M., Levin, A., (2017), "Central Bank Digital Currency and the Future of Monetary Policy", NBER Working Paper No. 23711, National Bureau of Economic Research, Cambridge, Massachusetts.

Bofinger, P., (2018), "Digitalisation of money and the future of monetary policy", CEPR Policy Research.

Boston Consulting Group, (2018), "An Interactive Guide to Global Payments", see BCG homepage.

Buck, J., (2017), "Dubai will issue first ever state cryptocurrency", Cointelegraph, 1, October 2017.

Campell, H. R., "Cryptofinance" Online Course Material, Duke University, Durham.

Committee on Payment and Settlement Systems, Technical Committee of the International Organization of Securities Commissions, (2012), "Principles for financial market infrastructures", Bank for International Settlements, Basel, Switzerland:

Committee on Payments and Market Infrastructures, (2015), "Digital Currencies", Bank for International Settlements, Basel, Switzerland.

Committee on Payments and Market Infrastructures, (2016), "Correspondent Banking", Bank for International Settlements, Basel, Switzerland.

Committee on Payments and Market Infrastructures, (2017), "Distributed Ledger Technology in Payment, Clearing and Settlement", Bank of International Settlements, Basel, Switzerland.

Committee on Payments and Market Infrastructures, (2018), "Central bank digital currencies", Bank for International Settlements, Basel, Switzerland.

Creswell, J., W., Creswell, J., D., (2018) "Research Design: Qualitative, Quantitative, and Mixed Methods Approaches", Sage Publications Ltd.

Diehl, M., Alexandrova-Labadjova, B., Heuver, R., Martinez-Jaramillo, S., (2015) “Analysing the Economics of Financial Market Infrastructures” IGI.

Directive (EU) 2015/2366 of the European Parliament and of the Council on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

Davoodalhosseini, M., Rivadeneyra, F., (2018), ‘A Policy Framework for E-Money: A Report on Bank of Canada Research”, Bank of Canada Staff Discussion Paper 2018-5, April 2018.

Esselink, H., Hernandez, L., (2017), ‘The use of cash by households in the euro area ‘, ECB Occasional Paper no 201, European Central Bank.

European Association for Secure Transactions (EAST), (2016), “European ATM Crime Report, January – June 2016”.

European Central Bank, (2012) “Virtual currency schemes”, Eurosystem.

European Central Bank, (2015), “Virtual currency schemes – a further analysis”, Eurosystem.

European Commission DG Competition, (2015), “Survey on merchants costs of processing cash and card payments”, March 2015.

European Parliament Economic and Monetary Affairs Committee, (2017), “The Implications of Digital Currencies for Monetary Policy”, Monetary Dialogue.

European Parliament Economic and Monetary Affairs Committee, (2016), “Report on virtual currencies”.

Francioni, R., Schwartz, R.A., (2017). “Equity Markets in Transition: the value chain, price discovery, regulation, and beyond”, Springer International Publishing, Switzerland.

Financial Stability Board, (2017), “Correspondent Banking Data Report”, July 2017.

Financial Stability Board, (2018), “Progress Report on Correspondent Banking and Remittances”, March 2018.

European Banking Authority, (2014), “Opinion on virtual currencies”.

Fung, B., Halaburda, H., (2016), “Central Bank Digital Currencies: A Framework for Assessing Why and How”, Staff Discussion Paper 2016-22, Bank of Canada.

Gandal, N., Hamrick, J.T., Moore, T., Oberman, T., (2018), “Price manipulation in the Bitcoin ecosystem”, Journal of Monetary Economics 95: 86-96.

Garcia, F.D., Hoepman, J. H., (2005), “Off-line Karma: A Decentralised Currency for Static Peer-to-Peer and Grid Networks”, Applied Cryptography and Network Security, 364-377.

Gray, S.T., (2006), “Central Banking in Low Income Countries”, Lecture Series No. 5, Centre for Central Banking Studies, Bank of England, London.

Grinberg, R., (2012) “Bitcoin: An Innovative Alternative Digital Currency”, Hastings Science and Technology Law Journal 4(1) (Winter): 159-207.

Grolleman, D. J., Jutrsa, D., (2017), “Understanding Correspondent Banking Trends: A Monitoring Framework”, IMF Working Paper, WP/17/216.

Hayek, F., (1976), “The Denationalization of Money”, London: Institute of Economic Affairs.

Heikkinen, P., Grym, A., Kauko, K., Takala, K., (2017), “Central Bank Digital Currency”, Bank of Finland Economics Review, No. 5, 2017.

Hilemann, G. and Rauchs, M., (2017), “Global Cryptocurrency Benchmarking Study”, Research Study, University of Cambridge Judge Business School and Cambridge Centre for Alternative Finance, Cambridge.

Holthausen, C., Rønde, T., (2002) "Regulating Access to International Large-Value Payment Systems", Review of Financial Studies, 15, 1561-1586.

International Monetary Fund, (2018), "Casting Light on Central Bank Digital Currency", Staff Discussion Note 18/08, November 2018, IMF.

International Monetary Fund, (2017), "Recent trends in correspondent banking relationships – Further Considerations", IMF.

International Monetary Fund (collective of authors), (2016), "Virtual currencies and beyond: initial considerations", IMF.

Jensen, H., F., (2017), "Central Banks and digital currencies – a solution without problems?", speech given at the Official Monetary and Financial Institutions Forum, London, 30. October 2017.

Jevons, W., S., (1876), "Money and the Mechanism of Exchange", D. Appleton and Co. Publishers, New York, 1876.

Kahn, C. M., (2018), "The threat of privacy", Journal of Financial Market Infrastructures 6 (2/3), pp. 1-10.

Kahn, C. M., Roberds, W., (2001), "Real-time gross settlement and the costs of immediacy", Journal of Monetary Economics 47, 299–319.

Kahn, C. M., Roberds, W., (2002), "The Economics of Payment Finality", Economic Review Second Quarter 2002, Federal Reserve Bank of Atlanta.

Kahn, C. M., Roberds, W., (2006a), "Transferability, finality, and debt settlement", Journal of Monetary Economics 54, 955–978.

Kahn, C. M., Roberds, W., (2006b), "Why pay? An introduction to payment economics", Journal of Financial Intermediation 18, 1-23.

Kahn, C. M., Roberds, W. (2009) "Payments Settlement: Tiering in Private and Public Systems" Journal of Money, Credit and Banking, Vol.41, No.5 (August 2009). 855-884.

Kahn, C. M., McAndrews, J. J., Roberds, W., (2003), “Settlement risk under net and gross settlement”, Journal of Money, Credit and Banking 47, 299–319.

Kahn, C.M., McAndrews, J., Roberds, W., (2005), “Money is privacy”, International Economic Review, Vol. 46, No. 4, pp. 432-53.

Karame, G. O., Androulaki, E., Čapkun, S., (2012) “Double-spending Fast Payments in Bitcoin. In Proceedings of the 2012”, ACM Conference on Computer and Communications Security, 906-917.

King, M., (2016), “The End of Alchemy: Money, Banking, and the Future of the Global Economy”, W.W. Norton and Company, London.

Köppl, T., Monnet, C., Temzelides, T., (2008), “A Dynamic Model of Settlement”, Journal of Economic Theory, 142, 223-246.

Kokkola, T., (2010), “The Payment System: Payments, Securities and Derivatives, and the Role of the Eurosystem”, European Central Bank.

Kumhof, M., Noone, C., (2018), “Central bank digital currencies – design principles and balance sheet implications”, Staff Working Paper No. 725, Bank of England.

Koning, J., (2014), “Fedcoin”, Moneyness, blog post, 19 October 2014.

Lagarde, C., (2017), “Central Banking and Fintech – a brave new world?”, Speech at the Bank of England, 30.09.2017, IMF.

Lagarde, C., (2018), “Winds of Change: The Case for New Digital Currency”, Speech at the Singapore Fintech Festival, 14.11.2018, IMF.

Lamport, L., Shostak, R. and Pease, M., (1982), “The Byzantine Generals Problem”, ACM Transactions on Programming Language and Systems, Vol. 4, No. 3, 382 – 401.

Lastra, R. M., Allen, J. G., (2018), “Virtual currencies in the Eurosystem: challenges ahead”, Policy Department for Economic, Scientific and Quality of Life Policies, Directorate-General Internal Policies, European Parliament.

Lawrence, L., (1997), “An Introduction to Payment Systems”, Aspen Publishers, New York.

Lester, B., Millard, S., Willison, M., (2006) “Optimal settlement rules for payment systems”, Paper presented at the Economics of Payments, Federal Reserve Bank of New York.

McAndrews, J. J., Trundle, J., (2001), “New payment system design: Causes and consequences”, Bank of England Financial Stability Review 11, 127–136.

McAndrews, J.J., (2017), “The case for cash”, Asian Development Bank Institute Working Paper Series, No. 679.

McCorry, P., Shahandashti S.F., Hao F., (2016), “Refund attacks on Bitcoin’s Payment Protocol”, School of Computing Science, Newcastle University UK.

McCallum, B., T., (2000), “Theoretical Analysis Regarding a Zero Lower Bound on Nominal Interest Rates”, NBER Working Paper No. 7677, April 2000.

McKinsey, (2016), “Global Payments 2016: Strong Fundamentals despite Uncertain Times”, McKinsey&Company, Financial Services Practice.

Meaning, J., Dyson, B., Barker, J., Clayton, E., (2018), “Broadening narrow money: monetary policy with a central bank digital currency”, Staff Working Paper 724, Bank of England.

Mersch, Y., (2017 (1)), “Why Europe still needs cash”, contribution by Yves Mersch for Project Syndicate, European Central Bank.

Mersch, Y., (2017 (2)), “Digital base money: an assessment from the ECB’s perspective”, paper presented at the farewell ceremony for Pentti Hakkarainen, Deputy Governor of Suomen Pankki — Finlands Bank, Helsinki, 16th January.

Milne, A., (2017), "Cryptocurrencies from an Austrian perspective", School of Business and Economics, Loughborough University.

Moore, G. E., (1965), "Cramming more components into electronic circuits", Electronics, Volume 38, No. 8, 19. April 1965.

Nakamoto, S., (2008), "Bitcoin: A Peer-to-Peer Electronic Cash".

Nosal, E., Rocheteau, G., (2006), "The economics of payments", Policy discussion paper No. 14, Federal Reserve Bank of Cleveland.

Olsen, O., (2018), "Central Bank digital currencies", Norges Bank Papers, No. 1, 2018.

Ongaro, D., Ousterhout, J., (2014), "In search of an understandable consensus algorithm", Stanford University.

Pagès H., Humphrey D., (2005) "Settlement finality as a public good in large-value payment systems", ECB Working Paper, No 506/ July 2005.

Peters G. W., Panayi E., Chapelle A., (2015), "Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective", UCL, Oxford University, LSE.

Pieters, G. C., (2017), 'The Potential Impact of Decentralized Virtual Currency on Monetary Policy", Federal Reserve Bank of Dallas, Globalization and Monetary Policy Institute 2016 Annual Report.

Project Jasper, (2017), "A Canadian experiment with distributed ledger technology for domestic interbank payments settlement", White Paper prepared by Payments Canada, R3 and the Bank of Canada.

PwC, (2017), "Redrawing the Lines: FinTech's Growing Influence and Financial Services", Global Fintech Report 2017.

PYMTS.com, Cardtronics, (2016), "Global Cash Index", www.pymts.com

Riksbank, (2017 (1)), "The Riksbank e-krona project, Report 1", Stockholm, September 2017.

Riksbank, (2017 (2)), “Riksbanken’s e-krona Project plan — phase 1”, Stockholm, 14th March.

Schmidt, T., (2016), „Barzahlen in Deutschland beliebter als in anderen Ländern“, Bundesbank Research Brief, Deutsche Bundesbank, Frankfurt am Main.

Schmiedel, H., Kostova, G., Ruttenberg, W., (2012), “The social and private costs of retail payment instruments, a European perspective”, Occasional Paper Series, No. 137, 43, European Central Bank.

Seventh T2S Harmonisation Progress Report, (2017), T2S Advisory Group, European Central Bank.

Shadab, H. B., (2014), “Regulating Bitcoin and Block Chain Derivatives”, New York Law School, Written statement to the Commodity Futures Trading Commission Global Markets Advisory Committee, October 9, 2014.

Swan, M., (2015) “Blockchain: Blueprint for a new economy”, Sebastopol: O’Reilly.

SWIFT, (2018), “gpi real-time Nostro Proof of Concept”, SWIFT.

The Wolfsberg Group, (2014), “Wolfsberg Anti-Money Laundering Principles for Correspondent Banking”.

The World Bank, (2015), “Withdrawal from Correspondent Banking. Where, Why, and What to do about it”, Finance and Markets Global Practice, The World Bank Group.

Tilson D., Lyytinen K., Sorensen C., (2010), “Desperately Seeking the Infrastructure in IS Research Conceptualization of Digital Convergence As Co-Evolution of Social and Technical Infrastructures”, System Sciences (HICSS), 1-10.

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

Untiset, (2016), “Bank of Finland predicts country will be cash-free by 2029”, 21.02.2016.

Wandhöfer, R., (2010) “EU payments integration: SEPA, PSD and other milestones along the road”, London: Palgrave MacMillan.

Wandhöfer, R., Berndsen, R. J., (2018), “Proof-of-Work blockchains and Settlement Finality: a functional interpretation?”, (forthcoming publication).

Van Hove, L., (2015), “Cash note printing in a less-cash society: innovate or not?”, Risk.net publication, September 2015.

Zapfel, R., (2019), “DRME – a asynchronous distributed random leader election for consensus in a small-scale network of well-known processes”, Patent Application Reg. No. 19 450 001 3, Austrian Patent Office.