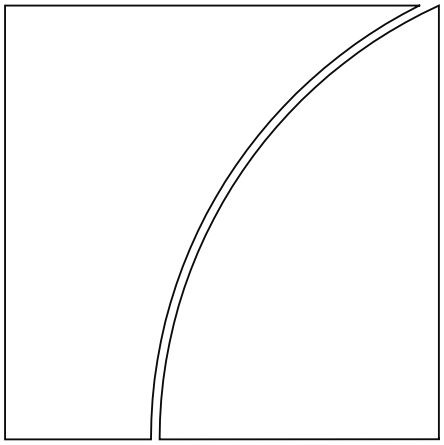
Committee on Payments and Market Infrastructures



Digital currencies

November 2015

BANK FOR INTERNATIONAL SETTLEMENTS

This publication is available on the BIS website (www.bis.org).

ISBN 978-92-9197-384-2 (print)
ISBN 978-92-9197-385-9 (online)

Contents

Executive summary

Central banks typically take an interest in retail payments as part of their role in maintaining the stability and efficiency of the financial system and preserving confidence in their currencies. Innovations in retail payments can have important implications for safety and efficiency; accordingly, many central banks monitor these developments. The emergence of what are frequently referred to as "digital currencies" was noted in recent reports by the Committee on Payments and Market Infrastructures (CPMI) on innovations and non-banks in retail payments. A subgroup was formed within the CPMI Working Group on Retail Payments to undertake an analysis of such "currencies"[1] and to prepare a report for the Committee.

The subgroup has identified three key aspects relating to the development of digital currencies[2]. The first is the assets (such as bitcoins) featured in many digital currency schemes. These assets typically have some monetary characteristics (such as being used as a means of payment), but are not typically issued in or connected to a sovereign currency, are not a liability of any entity and are not backed by any authority. Furthermore, they have zero intrinsic value and, as a result, they derive value only from the belief that they might be exchanged for other goods or services, or a certain amount of sovereign currency, at a later point in time. The second key aspect is the way in which these digital currencies are transferred, typically via a built-in distributed ledger. This aspect can be viewed as the genuinely innovative element within digital currency schemes. The third aspect is the variety of third-party institutions, almost exclusively non-banks, which have been active in developing and operating digital currency and distributed ledger mechanisms. These three aspects characterise the types of digital currencies discussed in this report.

A range of factors are potentially relevant for the development and use of digital currencies and distributed ledgers. Similar to retail payment systems or payment instruments, network effects are important for digital currencies, and there are a range of features and issues that are likely to influence the extent to which these network effects may be realised. It has also been considered whether there may be gaps in traditional payment services that are or might be addressed by digital currency schemes. One potential source of advantage, for example, is that a digital currency has a global reach by design. Moreover, distributed ledgers may offer lower costs to end users compared with existing centralised arrangements for at least some types of transactions. Also relevant to the emergence of digital currency schemes are issues of security and trust, as regards the asset, the distributed ledger, and the entities offering intermediation services related to digital currencies.

This report considers the possible implications of interest to central banks arising from these innovations. First, many of the risks that are relevant for e-money and other electronic payment instruments are also relevant for digital currencies as assets being used as a means of payment. Second, the development of distributed ledger technology is an innovation with potentially broad applications. Wider use of distributed ledgers by new entrants or incumbents could have implications extending beyond payments, including their possible adoption by some financial market infrastructures (FMIs), and more broadly by other networks in the financial system and the economy as a whole. Because of these

[1] Although "digital currencies" typically do have some, but not all the characteristics of a currency, they may also have characteristics of a commodity or other asset. Their legal treatment can vary from jurisdiction to jurisdiction. Use of the term "digital currencies" in the report is not meant to indicate any particular view of what digital currencies are or what policy towards them should be.

[2] A further note on terminology: this report uses the term "digital currencies", because, while recognising that the term is not perfect, the term is used widely and reflects the concept that these are assets that are represented in digital form. Previous CPMI reports used the term "virtual currencies", reflecting their existence in a virtual rather than physical form; virtual currencies in particular are prevalent in certain online environments. Moreover, these schemes are frequently referred to as "cryptocurrencies", reflecting the use of cryptography in their issuance, and in the validation of transactions.

considerations, it is recommended that central banks continue monitoring and analysing the implications of these developments, both in digital currencies and distributed ledger technology.

1. Introduction

Digital currencies, and especially those which have an embedded decentralised payment mechanism based on the use of a distributed ledger,[3] are an innovation that could have a range of impacts on various aspects of financial markets and the wider economy. These impacts could include potential disruption to business models and systems, as well as facilitating new economic interactions and linkages. In particular, the potential implications of digital currencies and distributed ledgers on retail payment services seem to be especially important, as these schemes have the potential to facilitate certain retail payment transactions (eg for e-commerce, cross-border transactions and person-to-person payments), and possibly make them faster and less expensive for end users such as consumers and merchants. However, the implications for payment system efficiency are still to be determined, and potential risks may arise from the operation of these schemes. In addition, they may also raise a number of policy issues for central banks and other authorities. In the near term, the policy issues for central banks are likely to centre on the payment system implications. However, should digital currencies and distributed ledgers become widely used (potentially also for large-value transactions or for other asset types beyond funds transfers), their impact on other areas of responsibility for central banks, such as payment system oversight and regulation, financial stability and monetary policy, might become more prominent.

Currently, digital currency schemes are not widely used or accepted, and they face a series of challenges that could limit their future growth. As a result, their influence on financial services and the wider economy is negligible today, and it is possible that in the long term they may remain a product for a limited user base on the fringes of mainstream financial services. However, the operation of some digital currency schemes in recent years indicates the feasibility of using distributed ledgers for peer-to-peer value transfers in the absence of a trusted third party. As such, various features of distributed ledger technology may have potential to improve some aspects of the efficiency of payment services and financial market infrastructures (FMIs) in general. In particular, these improvements might arise in circumstances where intermediation through a central party is not currently cost-effective.

The Committee on Payments and Market Infrastructures (CPMI) has a mandate to promote "the safety and efficiency of payment, clearing, settlement and related arrangements, thereby supporting financial stability and the wider economy."[4] The CPMI's focus extends beyond FMIs and includes, inter alia, retail payment instruments or schemes, both within and across jurisdictions. Retail payments play a key role within both the financial system and the rest of the economy and they have been subject to particular attention by the CPMI, reflecting the interest of member central banks in this issue. Recent work of the CPMI in this field includes the reports *Innovations in retail payments* (2012) and *Non-banks in retail payments* (2014). In the latter report, decentralised digital currencies were briefly discussed.

Taking into account the CPMI's mandate and the potential implications of digital currencies and distributed ledgers in these areas, the CPMI agreed in November 2013 that there was a need to closely monitor new developments in this field. In February 2015, it was decided that the Working Group on Retail Payments would carry out further analytical work in the area of digital currencies. This report responds to the CPMI mandate and provides an initial analysis of the main factors influencing the development of digital currencies and distributed ledgers, as well as an overview of the potential implications, with a particular emphasis on the payment system implications.

The report is structured as follows: after this introduction, the second section provides an overview of the key features of digital currencies, including how they differ from traditional forms of electronic money (e-money); the third section elaborates on the main factors influencing the development

[3] The term "distributed ledger" is used throughout the document as this is a term commonly used to describe the main innovation that allows decentralised payment mechanisms to be implemented.

[4] Committee on Payments and Market Infrastructures (CPMI), Charter, September 2014, http://www.bis.org/cpmi/charter.pdf.

of digital currencies and distributed ledgers from both the demand and supply sides; the fourth section details some of the potential implications of these schemes should the degree of their acceptance increase substantially; finally, the fifth section identifies potential areas for further work. The report's first annex lists relevant documents published by CPMI central banks on digital currencies and distributed ledgers.

2. Key features and uses of digital currencies

Money denominated in a particular currency (money in a traditional sense) includes money in a physical format (notes and coins, usually with legal tender status) and different types of electronic representations of money, such as central bank money (deposits in the central bank that can be used for payments) or commercial bank money.

Electronic money (e-money), defined in the CPMI's *A glossary of terms used in payments and settlement systems* as "value stored electronically in a device such as a chip card or a hard drive in a personal computer", is also commonly used around the world. Some jurisdictions have developed specific legislation regulating e-money (eg the E-Money Directive in the EU). E-money balances according to the legislation applicable in a particular jurisdiction (e-money in a narrow sense) are usually denominated in the same currency as central bank or commercial bank money, and can easily be exchanged at par value for them or redeemed in cash. Since the mid-1990s, the CPMI has studied the development of e-money and the various policy issues associated with it.[5] These categories (cash, central or commercial bank money, and e-money in a narrow sense) are traditionally perceived as "money" in a specific currency, giving rise to a currency's single character.[6]

Subsequent definitions of e-money have widened the concept to include a variety of retail payment mechanisms, possibly extending to digital currency schemes. While digital currencies may meet the broad conceptual definition of e-money, in most jurisdictions they typically do not satisfy the legal definition of e-money. For example, in many jurisdictions, the value stored and transferred must be denominated in a sovereign currency to be considered e-money; however, in many cases digital currencies are not denominated in or even tied to a sovereign currency, but rather are denominated in their own units of value. In the case of the EU, the legal definition of e-money includes the requirement that the balances issued should be a claim on the issuer, issued on receipt of funds. Given this, units of digital currencies in some schemes will not be considered e-money in a legal sense as they are not issued in exchange for funds (even though they can be subsequently bought and sold), and may not be issued by any individual or institution.

Hundreds of digital currency schemes based on distributed ledgers currently exist, are in development or have been introduced and have subsequently disappeared. These schemes share several key features, which distinguish them from traditional e-money schemes.

First, in most cases, these digital currencies are **assets** with their value determined by supply and demand, similar in concept to commodities such as gold. However, in contrast to commodities, they have zero intrinsic value. Unlike traditional e-money, they are not a liability of any individual or institution, nor are they backed by any authority. As a result, their value relies only on the belief that they might be exchanged for other goods or services, or a certain amount of sovereign currency, at a later point in time. The establishment or creation of new units (ie the management of the total supply), is typically determined by a computer protocol. In those cases, no single entity has the discretion to manage the supply of units

[5] Bank for International Settlements (BIS), *Implications for central banks of the development of electronic money*, October 1996.

[6] For a detailed explanation of this perception of "singleness" in relation to central and commercial bank money (mainly based on the confidence that banks have the ability to convert their sight liabilities into central bank money upon demand), see CPMI, *The role of central bank money in payment systems*, August 2003.

over time – instead, this is often determined by an algorithm. Different schemes have different long-run supplies and different predetermined rules for the creation and issuance of new units. These predetermined rules help to create scarcity in the supply. These schemes tend not to be denominated in or tied to a sovereign currency, such as the US dollar or the euro. Using Bitcoin as an example, a bitcoin is the unit of value that is transferred.

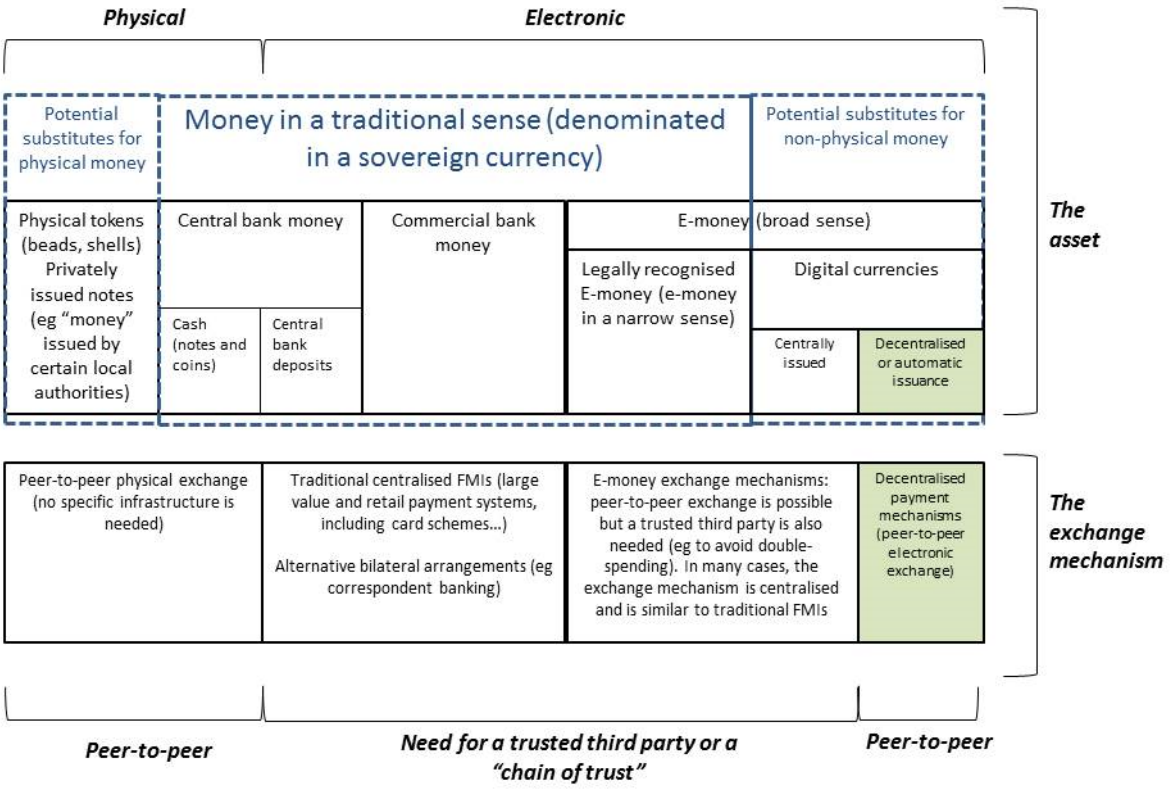
The second distinguishing feature of these schemes is the way in which value is transferred from a payer to a payee. Until recently, a peer-to-peer exchange between the parties to a transaction in the absence of trusted intermediaries was typically restricted to money in a physical format. Electronic representations of money are usually exchanged in centralised infrastructures, where a trusted entity clears and settles transactions. The key innovation of some of these digital currency schemes is the use of **distributed ledgers** to allow remote peer-to-peer exchanges of electronic value in the absence of trust between the parties and without the need for intermediaries. Typically, a payer stores in a digital wallet his/her cryptographic keys that give him/her access to the value. The payer then uses these keys to initiate a transaction that transfers a specific amount of value to the payee. That transaction then goes through a confirmation process that validates the transaction and adds it to a unified ledger of which many copies are distributed across the peer-to-peer network. The confirmation process for digital currency schemes can vary in terms of speed, efficiency and security. In effect, distributed ledgers replicate the peer-to-peer exchange of value, although on a remote basis over the internet.

Closely related to the way in which value is transferred is *the way in which transactions are recorded and in which value is stored*. As mentioned above, the transfer is completed when the ledger that is distributed across the decentralised network is updated. The amount of information that is stored in the ledger can vary from a bare minimum – such that the identity of payers and payees is difficult to ascertain and only the distribution of value across network nodes is kept – to a wealth of information that can include details about the payer, payee, transactions and balances. In many cases today, digital currency schemes require very little information to be kept in the ledger.

Another distinguishing feature of these schemes is their **institutional arrangements**. In traditional e-money schemes, there are several service providers that are essential to or embedded in the operation of an e-money scheme: the issuers of e-money, the network operators, the vendors of specialised hardware and software, the acquirers of e-money, and the clearer(s) of e-money transactions. In contrast, many digital currency schemes are not operated by any specific individual or institution (though some are promoted actively by certain intermediaries). This differs from traditional e-money schemes that have one or more issuers of value that represent liabilities on the issuers' balance sheets. Moreover, the decentralised nature of some digital currency schemes means that there is no identifiable scheme operator, a role that is typically played by financial institutions or other institutions that specialise in clearing in the case of e-money. There are a number of intermediaries, however, that supply various technical services. These intermediaries may provide "wallet" services to enable users of the digital currency to transfer value, or may offer services to facilitate the exchange between digital currency units and sovereign currencies, other digital currency units or other assets. In some instances, these intermediaries store the cryptographic keys to the value for their customers.

Figure 1 illustrates the separation between the two basic aspects of digital currency schemes (the asset side and the decentralised exchange mechanism based on a distributed ledger), and aims to provide a framework to help explain where e-money and digital currencies could be placed in relation to other types of money.

Taxonomy of money and exchange mechanisms Figure 1



The potentially disruptive innovations associated with digital currency schemes refer not only to the "asset aspect" (digital currencies issued automatically which are not a liability of any party), but more significantly to the "payment aspect" (payment mechanisms based on a distributed ledger that allow peer-to-peer transfers without the involvement of trusted third parties). While these two aspects are closely linked together in some digital currency schemes (eg Bitcoin), this is not necessary in all cases. There are different ways in which digital currencies and distributed ledgers could operate in principle, with differing degrees of interaction with existing infrastructures and payment service providers.

Some digital currency schemes based on a distributed ledger aim to create a network that would work in isolation from, or with only a marginal connection to, existing payment mechanisms. Users of the system would directly open accounts in a single distributed ledger and send and receive peer-to-peer payments denominated in the digital currency native to the network. The only connection with the existing payment system would arise in exchanges and trading platforms, where the digital currency units would be exchanged for sovereign currency, usually at free-floating rates that reflect supply and demand (minus a service fee charged by the exchanges/trading platforms).

In other instances, digital currencies based on distributed ledgers could be used by traditional payment service providers (such as banks) with the aim of improving the efficiency of certain processes. This could involve using distributed ledgers to set up a decentralised payment mechanism between payment system participants to improve back office clearing and settlement processes, whereas front office services between these service providers and end users might remain unaltered (end users might even be unaware that digital currencies and distributed ledgers are being used to complete a payment denominated in sovereign currency).

The use of distributed ledgers in isolation is also conceivable. Distributed ledgers could in principle be re-engineered and adapted to new or existing payment systems without necessarily involving the issuance of a digital currency (the distributed ledgers might in principle be adapted to be used with sovereign currency).

3. Factors influencing the development of digital currencies

Digital currencies based on the use of a distributed ledger represent a genuinely new development in the payments landscape. Nevertheless, many of the factors that have spurred the development of digital currencies have also stimulated innovation in more traditional payment methods. Reduced cost and increased speed, including in the areas of e-commerce and cross-border transactions, are some of the factors underpinning both digital currency development and broader payment system innovation. In particular, it is worth highlighting the role of technology in driving the development of digital currencies and other innovations. The CPMI report Innovations in retail payments (2012) identified technological advances as a key enabling factor for changes in payment services, with an impact on both the demand for and supply of these services.

However, a range of factors also exist that are more idiosyncratic to digital currencies based on distributed ledgers – particularly related to their decentralised attributes.

3.1 Supply side factors

On the supply side, the development of digital currencies based on the use of a distributed ledger has been mostly driven by **private sector non-banks**.[7] For the most part, banks have tended not to engage directly with digital currency intermediaries – indeed, some have sought to avoid interaction as a result of perceptions of risk and uncertainty over legal or compliance issues (such as AML/CFT). Only relatively recently have there been reports that private banks are exploring potential business opportunities arising from digital currencies and distributed ledgers – for example, by investing in companies that specialise in providing digital currency services, offering their customers interfaces to digital currency exchanges or exploring the use of decentralised ledgers for back office applications. When considering whether to implement such digital currency-linked services, banks, or any other participant involved, may need to assess whether such implementation might pose security challenges.

The drivers that have led these entities to develop digital currency schemes are also diverse, and underlie many of the differences in design between various initiatives. One distinction relates to commercial versus not-for-profit motives. Where **commercial motives** are the main driver, the entity might be seeking to earn profits from digital currency schemes in a number of different ways. These profits can come from the issuing of digital currency units (ie seigniorage-like revenue), from a capital gain on the digital currency units associated with the scheme and from transaction fees from payment intermediation. Digital currencies can also form part of a larger business model where the digital currency scheme is mainly created to generate revenues through the sale of other items or services.

A number of digital currency schemes based on distributed ledgers have been developed with particular **non-profit motives** in mind. These might include the utility gained from experimentation and innovation for its own sake, ideological motivations related to the desire to create and/or use alternative methods to existing financial infrastructure, or facilitating financial inclusion.

[7] A non-bank in this report is defined as "any entity involved in the provision of retail payment services whose main business is not related to taking deposits from the public and using these deposits to make loans": see CPMI, *Non-banks in retail payments*, September 2014.

Some of the supply side factors that may have an influence on the future development of digital currencies based on the use of a distributed ledger are:

- **Fragmentation**: Currently, more than 600 digital currencies are in circulation, with different protocols for transaction processing and confirmation, and with different approaches to the growth in the supply of digital currency units. This diversity may represent a barrier to the use and acceptance of these schemes, as fragmentation in various initiatives could be an obstacle to achieving the critical mass necessary to realise the network effects that are common to all payment networks.
- **Scalability and efficiency:** Due to their limited scale and acceptance, the number of transactions currently being processed in digital currency schemes is orders of magnitude smaller than those handled by widely used retail payment systems. It remains to be seen if and to what extent digital currency schemes would be able to evolve in order to process a significantly higher number of transactions. The increased efficiency of these schemes cannot be taken for granted; some of the most important digital currency schemes seem to be resource-intensive in terms of the energy and computing power required to process a small number of transactions. Improvements in processing power and speed and the tendency for computing and hardware costs to decrease imply that scalability and efficiency issues might be addressed over time. Other digital currency schemes purportedly require fewer resources to operate.
- **Pseudonymity:**[8] The degree of anonymity provided by some digital currency schemes may discourage a range of financial system participants from direct use or from providing facilities for digital currency use to their customers, as AML/CFT requirements may be difficult to satisfy in relation to digital currency transactions. It is important to note that digital currency transactions are typically observable on a public ledger and to the extent that they are not intentionally disguised (eg via so-called anonymisers or mixers), although aspects of these ledgers may be difficult to analyse.
- **Technical and security concerns:** Digital currencies based on the use of a distributed ledger have to build consensus among network participants to ensure the uniqueness of the ledger (ie that there is a single version of the ledger – with the history of transactions and balances – distributed across the network). The acceptance of digital currencies can be affected if differing versions of the ledger can coexist during long periods of time, or if the procedures to achieve consensus are flawed. Malicious actors may seek to profit by introducing fraudulent transactions into the ledger and inducing other participants to verify the falsified ledger.
- **Business model sustainability:** Building a sustainable business model in the long term might be a particular challenge for some digital currency schemes. In some cases, the incentives for certain actors that support the scheme (eg by verifying transactions and incorporating them into the ledger) are directly related to the issuance of the currency, which might be capped or decrease over time. At the same time, the cost incurred by those actors might be significant in some digital currency schemes. In those cases, it is an open question whether the right incentives will remain for the scheme to operate when the supply of new digital currency units diminishes or disappears. It is also possible that transaction fees could be raised to compensate for the loss of revenue in the form of new digital currency units, but this might affect demand and the long-term sustainability of the scheme. Notably, not all schemes follow the same model, and the costs associated with the operation of the network and transaction fees vary across different initiatives.

It needs to be emphasised that, to a large extent, these factors seem more related to the procedures and specific technical implementations of the various digital currency schemes than to the

[8] Digital currency schemes based on distributed ledgers are typically described as enabling "pseudonymous" rather than anonymous transactions, since the distributed ledger is generally publicly available and may facilitate tracing a transaction recorded on the ledger to a particular counterparty.

broader concept of distributed ledgers. Competing schemes, all of them based on distributed ledger technologies, may have differing degrees of efficiency, anonymity or technical security, or may follow diverging business models depending on their design.

3.2 Demand side factors

In order to increase acceptance and use, digital currencies based on distributed ledgers have to provide end users with benefits over traditional services. Some of the potential factors that could have an influence in the evolution of demand for digital currencies and their related payment mechanisms are:

- **Security:** An important demand side factor in relation to the use of digital currencies based on distributed ledgers is the risk of loss for users. Security breaches may undermine users' confidence in the digital currency scheme – these may not only involve the scheme itself but also may affect the intermediaries that an end user deals with in order to transact with digital currency units. Somewhat analogous to cash, if a user loses specific information that provides him/her with "ownership" of digital currency units stored in a distributed ledger, then those units are likely to be unrecoverable. Some users of digital currencies have relied upon intermediaries for holding and storing information relevant to their ownership of digital currency units, and so must trust these intermediaries to mitigate end user risk of loss from hacking, operational failures or misappropriation.
- **Cost:** It has been argued that digital currencies based on distributed ledgers may offer lower transaction fees than other payment methods. In some schemes, the processing of the payments is rewarded by newly issued units, which may also have the potential for earning "capital gains" measured in sovereign currency units, rather than by transaction fees. For this reason, digital currency schemes may be an attractive alternative for some individuals or entities, especially in cross-border payments that generally involve paying high fees to payment service providers. Additionally, transactions in these schemes do not require intermediaries to facilitate payments, which might have a bearing on processing costs. However, the transaction costs in these schemes are not always transparent, and other costs may exist, such as conversion fees between the digital currency and a sovereign currency if the user does not wish to maintain balances denominated in digital currency units.
- **Usability:** Ease of use is generally critical for the adoption of payment methods and mechanisms, and can reflect factors such as the number of steps in the payment process, whether this process is intuitive and/or convenient and the ease of integration with other processes. Use of digital currencies and distributed ledgers may depend on some usability advantages compared with existing methods. Currently, many providers are trying to improve and facilitate the user's experience in digital currency schemes.
- **Volatility and risk of loss:** If users choose to hold the digital currency asset received as payment then they may face costs and losses associated with price and liquidity risks. These risks are not insubstantial given the volatility and market dislocations that have been witnessed for some of the better known digital currency schemes. While some users have sought to make speculative gains from this volatility, for most the variability of exchange rates can represent an obstacle to wider adoption. The extent to which price volatility would diminish if digital currency schemes were widely used is an open question, as is the long-run risk of loss from holding digital currencies with zero intrinsic value.
- **Irrevocability:** Digital currency schemes based on a distributed ledger often lack dispute resolution facilities and offer irrevocability of the payment, which reduces the payee's risk of having the payment reversed due to fraud or chargebacks. While this feature may be attractive for payees (such as merchants), it could also deter adoption and use by payers (such as consumers).

- **Processing speed:** It has been argued that digital currencies based on distributed ledgers have the potential to clear and settle transactions faster than traditional systems, although the processing speed of the various schemes varies according to their technical details. However, it should be noted that a range of innovations unrelated to digital currencies – such as faster retail payment systems – are also aiming to address this increasing demand for improved payment speed. Additionally, real-time gross settlement systems already underpin the wholesale financial markets and provide capabilities for very fast payment and settlement of large-value payments.
- **Cross-border reach:** Digital currencies based on distributed ledgers are basically open networks with a global scope. These schemes do not distinguish between users based on location, and therefore allow value to be transferred between users across borders. Moreover, the speed of a transaction is not conditional on the location of the payer and payee. Further, in the context of restrictions that may be placed on cross-border transactions by national authorities, the decentralised nature of these digital currency schemes means that it is difficult to impose such restrictions on transactions.
- **Data privacy/pseudonymity:** Some digital currency schemes based on distributed ledgers have the scope to allow transactions to be made without disclosing personal details or sensitive payment credentials (although this is not an essential feature of distributed ledgers). The attractiveness of pseudonymity and the avoidance of banks and authorities may be partly driven by the desire to circumvent laws and regulation. In this respect, combined with their global reach, digital currency schemes are potentially vulnerable to illicit use. However, there are also legitimate reasons why users may prefer to use anonymous payment methods (eg when the payee is not trusted to protect the information disclosed: this may arise in person-to-person online sales where the parties commonly have no previous experience of interaction).
- **Marketing and reputational effects:** Digital currency schemes based on distributed ledgers are widely viewed as an innovative and interesting payment method. At the margin, merchants may see benefits in accepting payments through a digital currency scheme to the extent that it boosts demand for their goods and services. Similarly, users may be attracted to these schemes due simply to the newness of the technology.

These factors are relevant not only for direct use of digital currencies and distributed ledgers by end users, but potentially also for indirect use (eg when a payment service provider uses a digital currency scheme as its back-end payment infrastructure).

3.3 Role of regulation

Regulatory arrangements may have an influence on the development and use of digital currencies. In general, the recent development of digital currencies and the novelty of their design mean that they may not be specifically regulated and do not fit easily into existing regulatory definitions and structures. Indeed, the borderless online nature of digital currencies, and the absence of an identifiable "issuer" of the instrument, pose particular challenges to attempts at regulation that a national authority might make (although other identifiable third-party providers might be more easily regulated).

Borderless, online and generally unregulated systems do not involve layers of correspondent banks and can potentially make transactions faster, more convenient and feasible at lower cost. On the other hand, these types of system have also raised important concerns by law enforcement authorities about the use of these systems for illegal activity, as well as compliance with AML/CFT obligations that apply to traditional payment methods and intermediation. The Financial Action Task Force (FATF) has published a range of reports on digital currencies. In 2014, it published an extensive report on digital currency issues, noting that "convertible virtual currencies that can be exchanged for real money or other

virtual currencies are potentially vulnerable to money laundering and terrorist financing",[9] while more recently it published guidance on a risk-based approach to virtual currency payments products and services, observing that establishing some guidance across jurisdictions treating similar products and services consistently according to their function and risk profile is essential for enhancing the effectiveness of the international AML/CFT standards.[10]

Regulation naturally imposes costs on payment system providers and intermediaries; digital currency providers may benefit from not being subject to these costs. Regulatory costs may arise in particular from obligations placed upon the issuer of a payment or financial instrument; several countries have begun to adjust existing regulations or pass new regulations to address concerns of law enforcement and other authorities. Some developers and users of digital currencies have opposed such developments, seeing them as inconsistent with the emergence of new technologies that are less regulated than the traditional payments industry. Others have seen lack of regulation as an impediment to the growth of public confidence in digital currencies, as some actors may refrain from investing in this new technology due to legal uncertainty and/or lack of protection for users.

In this context, the main types of regulatory responses to the challenge of digital currencies are explored in Box 1.

[9] Financial Action Task Force, *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*, June 2014.

[10] Financial Action Task Force, *Guidance for a Risk-Based Approach to Virtual Currencies*, June 2015.

Box 1

Regulatory issues and approaches

Regulatory issues for digital currencies based on distributed ledgers cover three main fields: consumer protection**,** prudential and organisational rules for the different stakeholders, and specific operating rules as payment mechanisms (eg settlement finality as in EU regulation).

Given the nature of digital currencies, which are typically online and therefore not limited to national jurisdictions, a coordinated approach at a global level may be important for regulation to be fully effective. However, this does not preclude certain actions at the national level, for which at least five general categories of actions can be identified:

- *Information/moral suasion*: rather than interfering directly with the development of digital currencies, authorities could decide to use moral suasion towards users and investors in order to highlight the relevant risks and to influence the market.
- *Regulation of specific entities*: via such an institutional approach, authorities could establish a limited set of regulations for specific types of entity (eg those that enable interaction between digital currencies and traditional payment instruments and/or the real economy). Firms that might be subject to specific regulation include intermediaries providing digital currency-related services such as exchanges, merchant acceptance facilities and "digital wallet" applications enabling users to store and transact in their units of the digital currency.
- *Interpretation of existing regulations*: some authorities may be able to assess whether existing regulatory arrangements might be applied to digital currencies and digital currency intermediaries. One example is in the area of taxation law, where authorities have made determinations of how tax legislation might apply to digital currency arrangements.
- *Broader regulation*: although jurisdictional issues are likely to be a challenge, authorities might seek to take a broader approach to regulation, potentially reflecting a functional approach such that regulatory obligations that apply to traditional payment methods and intermediaries also apply to digital currency schemes and digital currency intermediaries. As an example, authorities might seek to ensure that AML/CTF requirements apply to digital currency transactions and counterparties, or that the same consumer protection arrangements apply to transactions conducted with digital currencies as to other payment methods used by consumers.
- *Prohibition*: authorities could seek to ban the use of digital currencies in their respective jurisdictions. Practically, this could imply a ban on any digital currency-based financial activities, as well as digital currency exchanges or digital currency acceptance by retailers.

These categories can provide a general framework for the analysis and classification of actions undertaken by national authorities. Table 1 gives an overview of that classification, based on inputs from CPMI members (*Note: the following table does not attempt to provide a comprehensive overview of the current situation*).

Broad classification of the main types of regulatory action Table 1

Main options	Type of actions / Country examples
Information/moral suasion	• Public warnings • Investor/buyer information • Research papers *Most countries have issued these types of warnings, research or information notes.*
Specific stakeholder regulation	• Regulation of digital currency administrators (record-keeping, reporting, AML/TF). *Example: United States.* • Regulation of digital currency exchangers (record-keeping, reporting, prudential measures, AML/TF). *Examples: United States, France, Canada, Singapore, Sweden.* • Consumer protection measures (payment guarantee, redeemability etc).
Interpretation of existing regulations	• Application of regulation based on "interpretation" of how existing framework (eg tax law treatment) may be applied to digital currencies or digital currency intermediaries. *Example: United States*.
Overall regulation	• Dedicated regulation, covering all three aspects (consumer protection, prudential/organisational rules for stakeholders, and specific operating rules as payment systems).
Prohibition	• Ban (or amount cap) on retail Bitcoin transactions. • Ban on digital currency acceptance by retailers. • Ban on digital currency-based financial instruments. *Examples: China, Belgium.* • Ban on digital currency exchangers. • Ban on Bitcoin transactions between banks. *Examples: China, Mexico.*[11]

4. Implications for central banks of digital currencies and their underlying decentralised payment mechanisms

The development of digital currencies based on the use of distributed ledgers raises a number of potential policy issues for central banks and other public authorities. Those of particular relevance to central banks stem from the central banks' role in the payment system, the extent to which they have supervisory responsibilities for institutions that may provide digital currency services themselves or provide clearing services to other firms that provide such digital currency services, their conduct of monetary policy, their issuance of physical currency and their role in maintaining financial stability.

Although some of these issues are relevant today, other issues arise not from what digital currencies and distributed ledgers are currently, but from what they represent – a technology for settling peer-to-peer payments without trusted third parties and that may involve a non-sovereign "currency". It is important to highlight that a *widespread* adoption of these schemes would need to take place for some implications to materialise. Notwithstanding the media interest that has tended to surround these

[11] The fact that banks in Mexico are not allowed to conduct transactions with digital currencies such as Bitcoin is not an explicit regulatory response to the emergence of this type of asset. Rather, it is a consequence of the fact that financial institutions in Mexico must restrict themselves to trading and operating the assets permitted by Mexican regulation – and digital currencies such as Bitcoin are not included in this list.

schemes, for the time being they are not widely used and thus their impact on the mainstream financial system is negligible. It is possible that these schemes may remain a niche product for a limited user base. If this is the case, most of the implications below would continue to be more theoretical than real. If, however, there is a widespread adoption of digital currencies or of distributed ledgers (also applied to sovereign currencies) with potential impacts on the operations and balance sheets of banks and even central banks, some of the implications below may materialise.

4.1 Implications stemming from central banks' role in the payment system

In their roles as operators and/or overseers of payment systems and other FMIs, and as catalysts of payment system development and innovation, central banks typically have a responsibility to promote safe and efficient payment systems. In particular, the safety of payment systems is often predicated on how well risks are managed; accordingly, this subsection focuses on the implications of risks that may arise from digital currencies based on distributed ledger technology, drawing upon a set of risks, most of which are inherent in retail payment systems.

One key risk that receives some attention relates to consumer protection. For example, projecting the future value of digital currencies is difficult. As mentioned earlier, most digital currencies are denominated in their own units of value, do not have intrinsic value but instead depend upon user perceptions of value, are not tied to a sovereign currency, and, in many cases, are not a liability of any person or institution. Therefore, their value is based solely on users' expectations that they can exchange these units for something else of value, such as goods and services, or sovereign currencies, at a later date. These expectations can change greatly, and introduce greater volatility and risk of loss in the value of the units than is typically observed in the value of sovereign currencies in foreign exchange markets.[12]

Another consumer protection issue is the risk of fraud. Most digital currencies are designed to mimic cash transactions and so are relatively anonymous. These currencies are typically stored in digital wallets. These wallets have specific security features that protect them, such as the use of cryptography, which requires specific codes to access the units of value in the wallets. If these codes are stolen, the units of value could be stolen from the wallets. Third-party service providers can offer end users wallet services and provide additional protection.

Like traditional retail payment systems, a digital currency's payment mechanism is also subject to various risks. Whereas in traditional retail payment systems these risks are usually faced by financial institutions, in digital currency schemes end users, as direct participants, may face those risks. In particular, digital currencies are subject to operational risk. The extent of this risk will depend on the design of the mechanism. Many digital currencies' payment mechanisms are designed such that an exact copy of the records of transactions and wallet balances are stored on many computers around the world. This differs from traditional retail payment systems, where these records are more centrally stored at trusted entities such as financial institutions. These different payment mechanisms may reduce some types of operational risk (eg the failure of a specific node in the network need not alter the overall functioning of the scheme), but may increase others (eg the potential for there to be divergence between nodes in the network in relation to the currently "agreed" version of the ledger).

The system's decentralised setup and its open and flexible governance structure mean that it may be difficult to anticipate possible disruptions (eg hacking attacks on exchange platforms). This, in turn, may have some influence on the exchange rate of the digital currency. Moreover, the governance structure of digital currencies and their payment mechanisms may impact design improvements and security

[12] Sovereign currencies may face similar issues, but a significant difference in relation to digital currency schemes is that, in the latter, there is not a credible monetary authority committed to maintaining the value of the currency. Additionally, laws and regulations enforce the acceptance of sovereign currency for repaying debts (eg sovereign currency is usually required for paying taxes).

enhancements. Typically, changes to the payment mechanism require some form of consensus building by the users, without a central entity or set of governance arrangements. The way in which consensus is achieved can vary by digital currency. As a result, on the one hand, there can be delays in improvements if the decision-making process takes too much time, leaving the system more vulnerable to certain types of operational risks or other risks of fraud. On the other hand, the open source character of digital currencies allows all interested parties to contribute to improving the protocol, incentivised by self-interest in the functioning of the digital currency.

Legal risk may also be present in digital currencies and their payment mechanisms. Because digital currencies are meant to mimic cash, payments are generally final and irrevocable as soon as they are confirmed. There may be no legal structure or clarity of rights and obligations of various parties involved in a transaction. For example, liability issues may not be clearly understood in the event of fraud, counterfeiting, loss or theft. Alternatively, consumer protection may be in place more generally but may be difficult to enforce. Third-party service providers that support the use of digital currencies may provide some clarity through contractual arrangements with users.

The institutional arrangements related to the payment mechanism may introduce some degree of settlement risk. Because digital currency transactions are meant to replicate cash transactions, settlement is generally quick, and in some cases, instantaneous. Most mechanisms are designed such that there is no extension of credit for settlement. Thus, on the surface, there may be little liquidity or credit risk introduced by the system. However, third-party institutions that provide support for the use of digital currencies may need to manage liquidity in digital currencies and one or more sovereign currencies, especially as end users load or empty their digital currency wallets through conversions to or from sovereign currencies. Thus, these institutions have to manage liquidity effectively in order to execute transactions on behalf of customers, possibly introducing some settlement risk into the system.

The relative anonymity of digital currencies may make them especially susceptible to money laundering and other criminal activities. The usefulness of a digital currency for such purposes will depend on how much record-keeping the mechanism maintains about the transactions, how involved third-party service providers are in the transactions, whether such third parties comply with anti-money laundering requirements, and how easy it is to move digital currency across borders and convert that currency into sovereign currency.

A deeper analysis of the details of distributed ledgers could provide more information about the impact of this technology on retail payment systems, their functioning and associated risks.

4.2 Implications for financial stability and monetary policy

Impact on financial market infrastructures

The distributed ledger technology underlying many digital currency schemes could have a much broader application beyond payments. Decentralised mechanisms that exchange value based on a distributed ledger technology alter the basic setup of aggregation and netting on which many FMIs rely. In particular, it is conceivable that distributed ledgers could have an impact on the pledging of collateral or on the registration of shares, bonds, derivatives trades and other assets. The use of distributed ledgers may also induce changes in trading, clearing and settlement as they could foster disintermediation of traditional service providers in various markets and infrastructures. These changes may result in a potential impact on FMIs beyond retail payment systems, such as large-value payment systems, central securities depositories, securities settlement systems or trade repositories. The development of "smart" contracts based on distributed ledger technology capable of executing payments under certain conditions may create the possibility of making variation margin payments on an individual contract basis. This could significantly alter how bilateral margining and clearing works today, with net positions and collateral pools.

Impact on broader financial intermediaries and markets

Digital currencies and technology based on distributed ledgers could, if widely used, challenge the intermediation role of current actors in the financial system, especially banks. Banks are financial intermediaries that fulfil a role as delegated monitor of borrowers on behalf of depositors. Banks also typically perform liquidity and maturity transformation in the channelling of money from depositors to borrowers. If digital currencies and distributed ledgers were to become widespread, any ensuing disintermediation might have an impact on the mechanisms for saving or accessing credit. It is unclear who would take up the roles of traditional financial intermediaries in an economy based on the use of these schemes or whether these services could be provided at all in such a context.

Implications for central bank seigniorage revenue

A widespread substitution of banknotes with digital currencies could lead to a decline in central bank non-interest paying liabilities. This, in turn, could lead central banks to substitute interest paying liabilities, reduce their balance sheets, or both. The result could be a reduction in central bank earnings that constitute central bank seigniorage revenue. This is also an issue that was analysed in depth in the context of the development of e-money. In particular, the previous analysis suggests a number of options that the central bank could consider to offset the loss of seigniorage revenue and to increase its balance sheet. A deeper analysis of the impact of digital currencies on seigniorage could build on this previous body of work. In any case, a substantial substitution would need to take place for any significant impact to materialise.

Implications for monetary policy

If the adoption and use of digital currencies were to increase significantly, the demand for existing monetary aggregates and the conduct of monetary policy could be affected, although at present, the use of private digital currencies appears too low for these risks to materialise. The impact of digital currencies in these areas would have many similarities with the potential impact of e-money. As discussed in depth in the 1990s[13], the effect of digital currencies on the implementation of monetary policy will depend on the change in demand for bank reserves (eg a substitution away from the existing banking system for deposits and payments, towards digital currencies) and the degree of economic and financial interconnection between the users of sovereign currency and the users of the digital currency. If the substitution is large and the interconnection is weak, then monetary policy may lose efficacy.

In addition, a significant expansion of digital currencies could also raise a number of technical issues regarding the appropriate definition of monetary aggregates, especially if the digital currencies were not denominated in the sovereign currency. In a monetary policy regime heavily focused on the growth of monetary aggregates, such measurement difficulties could create some complications for monetary policy implementation.

A deeper analysis of the possible impact of digital currencies and the broader use of distributed ledgers (also applied to sovereign currencies) could explore these issues in more detail.

4.3 Potential issuance of digital currency by central banks

The 1996 BIS report on e-money[14] contemplated central banks issuing e-money as a policy option in response to its widespread adoption by the public and the associated weakening of control over monetary policy and loss of seigniorage revenue.

[13] See eg BIS, *Implications for central banks of the development of electronic money*, October 1996.

[14] BIS, *Implications for central banks of the development of electronic money*, October 1996.

The distinction between digital currencies and e-money lies in the associated technological innovation and its impact on the concept of settlement. Settlement in this context means a common agreement that a transaction has taken place. E-money is technologically similar to existing payment systems in that a trusted central party operates a ledger to which everyone in the system refers; settlement still requires a trusted central entity.

The emergence of distributed ledger technology could present a hypothetical challenge to central banks, not through replacing a central bank with some other kind of central body but mainly because it reduces the functions of a central body and, in an extreme case, may obviate the need for a central body entirely for certain functions. For example, settlement might no longer require a central ledger held by a central body if banks (or other entities) could agree on changes to a common ledger in a way that does not require a central record-keeper and allows each bank to hold a copy of the (distributed) common ledger. Similarly, in some extreme scenarios, the role of a central body that issues a sovereign currency could be diminished by protocols for issuing non-sovereign currencies that are not the liability of any central institution.

This raises the question of how central banks could respond to an increasing use of distributed ledger technology to settle transactions. One option is to consider using the technology itself to issue digital currencies. In a sense, central banks already issue "digital currency" in that reserve balances now only exist in electronic form and are liabilities of the central bank. The question is whether such digital liabilities should be issued using new technology and be made more widely available than at present. This raises a wide range of questions, including the impact on the payments system, the privacy of transactions, the impact on private sector innovation, the impact on deposits held at commercial banks, the impact on financial stability of making a risk-free digital asset more widely available, the impact on the transmission of monetary policy, the technology which would be deployed in such a system and the extent to which it could be decentralised, and what type of entities would exist in such a system and how they should be regulated. Within the central bank community, the Bank of Canada and the Bank of England have begun research into a number of these topics.

5. Conclusions

Digital currencies and distributed ledgers are an innovation that could have a range of impacts on many areas, especially on payment systems and services. These impacts could include the disruption of existing business models and systems, as well as the emergence of new financial, economic and social interactions and linkages. Even if the current digital currency schemes do not persist, it is likely that other schemes based on the same underlying procedures and distributed ledger technology will continue to emerge and develop.

The asset aspect of digital currencies has some similarities with previous analysis carried out in other contexts (eg there is analytical work from the late 1990s on the development of e-money that could compete with central bank and commercial bank money). However, unlike traditional e-money, digital currencies are not a liability of an individual or institution, nor are they backed by an authority. Furthermore, they have zero intrinsic value and, as a result, they derive value only from the belief that they might be exchanged for other goods or services, or a certain amount of sovereign currency, at a later point in time. Accordingly, holders of digital currency may face substantially greater costs and losses associated with price and liquidity risk than holders of sovereign currency.

The genuinely innovative element seems to be the distributed ledger, especially in combination with digital currencies that are not tied to money denominated in any sovereign currency. The main innovation lies in the possibility of making peer-to-peer payments in a decentralised network in the absence of trust between the parties or in any other third party. Digital currencies and distributed ledgers

are closely tied together in most schemes today, but this close integration is not strictly necessary, at least from a theoretical point of view.

This report describes a range of issues that affect digital currencies based on distributed ledgers. Some of these issues may work to limit the growth of these schemes, which could remain a niche product even in the long term. However, the arrangements also offer some interesting features from both demand side and supply side perspectives. These features may drive the development of the schemes and even lead to widespread acceptance if risks and other barriers are adequately addressed.

There are different ways in which these systems might develop: either in isolation, as an alternative to existing payment systems and schemes, or in combination with existing systems or providers. These approaches would have different implications, but both could have significant effects on retail payment services and potentially on FMIs. There could also be potential effects on monetary policy or financial stability. However, for any of these implications to materialise, a substantial increase in the use of digital currencies and/or distributed ledgers would need to take place. Central banks could consider – as a potential policy response to these developments – investigating the potential uses of distributed ledgers in payment systems or other types of FMIs.

Annex 1: Relevant literature

Badev, A and M Chen (2014): "Bitcoin: technical background and data analysis", *Finance and Economics Discussion Series*, 2014–104, Board of Governors of the Federal Reserve System, December.

Bank of France (2013): "The dangers linked to the emergence of virtual currencies: the example of bitcoins", *Focus*, no 10, December, www.banque-france.fr/uploads/tx_bdfgrandesdates/Focus10-the_dangers_linked_to_the_emergence_of_virtual_currencies_the_example_of_bitcoins-GB.pdf.

Chiu, J and T-N Wong (2014): "E-money: efficiency, stability and optimal policy", Bank of Canada, *Working Paper*, 2014–16, April.

European Central Bank (2015): "Virtual currency schemes – a further analysis", February, www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf.

Fung, B, M Molico and G Stuber (2014): "Electronic money and payments: recent developments and issues", Bank of Canada, *Discussion Paper*, 2014–2, April.

Fung, B and H Halaburda (2014): "Understanding platform-based digital currencies", *Bank of Canada Review*, Spring, pp 12–20.

Gandal, N and H Halaburda (2014): "Competition in the cryptocurrency market", Bank of Canada, *Working Paper*, 2014–33, August.

Gans, J and H Halaburda (2013): "Some economics of private digital currency", Bank of Canada, *Working Paper*, 2013–38, November.

Reserve Bank of Australia (2014): *Submission to the inquiry into digital currency*, November, www.rba.gov.au/publications/submissions/inquiry-digital-currency-2014-11.pdf.

Robleh, Ali, J Barrdear, R Clews and J Southgate (2014): "Innovations in payment technologies and the emergence of digital currencies", Bank of England, *Quarterly Bulletin*, vol 54, no 3, September, pp 262–75.

——— (2014): "The economics of digital currencies", Bank of England, *Quarterly Bulletin*, vol 54, no 3, September, pp 276–86.

Sveriges Riksbank (2014): "What is Bitcoin?", *Sveriges Riksbank Economic Review*, no 2014:2, September, pp. 71–87, www.riksbank.se/Documents/Rapporter/POV/2014/2014_2/rap_pov_1400918_eng.pdf.

——— (2014): "Have virtual currencies affected the retail payments market?", *Economic Commentaries*, no 2, June, www.riksbank.se/Documents/Rapporter/Ekonomiska_kommentarer/2014/rap_ek_kom_nr-02_140617_eng.pdf.

Weber, W (2015): "Government and private e-money-like systems: Federal Reserve notes and national bank notes", Bank of Canada, *Working Paper*, 2015–18, June.

——— (2015): "The efficiency of private e-money-like systems: the US experience with national bank notes", Bank of Canada, *Working Paper*, 2015–3, January.

——— (2014): "The efficiency of private e-money-like systems: the US experience with state bank notes", Bank of Canada, *Working Paper*, 2014–15, April.

Annex 2: Members of the CPMI Working Group on Retail Payments

Bank of Mexico	Lorenza Martínez Trigueros (Chair)
Reserve Bank of Australia	David Emery
National Bank of Belgium	Jan Vermeulen
Central Bank of Brazil	Rogerio Antonio Lucca
Bank of Canada	Paul Miller
	Lana Embree
People's Bank of China	Chen Xue
European Central Bank	Francisco Tur Hartmann
	Emanuela Cerrato
Bank of France	Alexandre Stervinou
	Julien Lasalle
Deutsche Bundesbank	Heike Winter
	Johannes Klocke
Hong Kong Monetary Authority	Clarence Hui
	Helen Leung
Reserve Bank of India	Charulatha Kar
Bank of Italy	Maria Iride Vangelisti
	Michela Tocci
Bank of Japan	Shuji Kobayakawa
Bank of Korea	Eun Yeong Song
Bank of Mexico	Alberto Mendoza Hernández
Netherlands Bank	Jakob Rotte
Central Bank of the Russian Federation	Tatiana Mazgushina
Saudi Arabian Monetary Agency	Ali Al Homidan
Monetary Authority of Singapore	Chek Tchung Foo
South African Reserve Bank	Annah Manganyi
Bank of Spain	Carlos Conesa (since August 2015)
Sveriges Riksbank	Björn Segendorf
Swiss National Bank	David Maurer
	Nino Landerer
Central Bank of the Republic of Turkey	Ismail Behlul Kaya
Bank of England	Joanna Bibby-Scullion
Board of Governors of the Federal Reserve	David Mills
	Mark D. Manuszak
	Anjana Ravi

Federal Reserve Bank of New York	Antoine Martin
	Rodney Garratt
World Bank	Harish Natarajan
Secretariat	Carlos Conesa (until July 2015)
	Yuuki Shimizu

The report on digital currencies has also benefited significantly from the contributions of Clare Noone (Reserve Bank of Australia), Ben Fung and Scott Hendry (Bank of Canada), Robleh Ali and Emily Clayton (Bank of England), Iddo de Jong (European Central Bank), Paul Capocci (Bank of France), Prachi Gangrade (Reserve Bank of India), Eika Yamaguchi (Bank of Japan), Javier Perez-Estrada (Bank of Mexico), Jeffrey Marquardt (Board of Governors of the Federal Reserve System), Vanessa Kargenian (Federal Reserve Bank of New York), Thomas Lammer (The World Bank), Klaus Löber, Emanuel Freire (since August 2015) and Tze Hon Lau (Secretariat).