EUROPEAN CENTRAL BANK
EUROSYSTEM

Legal Working Paper Series

Phoebus Athanassiou

Impact of digital innovation on the processing of electronic payments and contracting: an overview of legal risks

No 16 / October 2017

Contents

Abstract

Digital innovations in finance have in recent years attracted strong interest from public authorities, financial sector stakeholders and academics alike, *inter alia* on account of their promise to reduce, or to altogether eliminate, the inefficiencies surrounding the execution and settlement of retail payments, including those linked to remote consumer transactions. For all the promises they hold, and their transformative potential, technological innovations also present challenges, some of which are of a legal nature. With technological innovation still at a formative stage, it is essential to identify and evaluate those challenges, so as to better understand which of their payment-specific applications to encourage (and how), and mitigate the risk of technological innovation destabilising the safety and efficiency of payments.

This paper seeks to explore the key legal issues that policy makers may wish to take into account in assessing the merits and risks of digital innovation, with an emphasis on its application to retail payments, and to contribute to an understanding of how technological advances are likely to affect both payment transactions and, no less importantly, the legal relationships between the parties to them.

The scope of this paper is limited to an examination of the legal implications of technological innovation for payments associated with consumer transactions, including those entered into online, and settled otherwise than by way of cash. Consequently, this paper will not examine the legal implications of technological innovation for the processing of transactions relating to transferable securities, for financial stability, for the conduct, by central banks, of their monetary policy operations, for the micro-prudential supervision of payment service providers, for competition among established payment service providers and new entrants, and for financial inclusion, issues of great legal and practical significance that merit (and, no doubt, will receive, going forward) specialized attention.

Keywords: FinTech, distributed ledgers, distributed ledger technologies, blockchain, virtual currencies, bitcoin, retail payments, smart contracts.

JEL codes: K24

1 Introduction

The volume of Internet-based retail consumer transactions (E-commerce) has been constantly growing in recent years, with an increasing number of consumers purchasing goods and services online.[1] While E-commerce has drastically changed the way in which consumers interact with traders it has not, yet, had as radical an impact on the actual *payment instruments* or *channels* for the final settlement of retail commercial transactions: these continue to be settled mostly through conventional means and, in particular, through bank transfers/direct debits and credit or debit cards.[2] This is despite the parallel emergence of single operator online payment platforms, mobile and contactless payments, which accounted for a smaller, but rising, share of the market for retail payments.[3]

Technology-enabled financial innovations (or 'FinTech') hold the promise[4] to transform the processing and settlement of retail payments in at least three distinct ways. The *first* is through the potential substitution of traditional means of payment by virtual currencies (VCs) and cryptocurrencies, such as *bitcoin*. The *second* is by tracking the processing of payments through decentralized (distributed) platforms (so-called 'distributed ledgers'), updated real-time, without the involvement of trusted third party intermediaries. And the *third* is by automating the execution and settlement of payment transactions through recourse to so-called 'smart contracts', written on distributed, digital platforms. For all their promises, digital innovations also pose a number of challenges, including legal and regulatory ones which, unless identified and overcome, are likely to undermine the prospects of FinTech as an enabler for reliable alternatives to established payment media and payment platforms.

This paper seeks to chart some of the legal issues to which the foregoing three types of financial innovation would appear likely to give rise, and their practical implications for payments and their recipients, mainly in a European Union (EU) context.

---

1 In 2015, the global E-commerce market was thought to have been worth USD 1.9 trillion, up by 14% compared to 2014. According to estimates, this figure will rise to USD 2.4 trillion by 2019 (source: *Worldpay*, 'Global Payments Report 2015', p. 9).

2 According to estimates, 2015 saw 25% of global payment transactions (by value) being settled by credit card, 17% by debit card and 10% by bank transfers (*Worldpay*, 'Global Payments Report 2016', p. 3).

3 According to estimates, 2015 saw 31% of global payment transactions (by value) being settled through E-wallets (*Worldpay*, 'Global Payments Report 2016', p. 3).

4 This promise is reflected in the considerable attention that digital innovation has attracted, in recent years, from the ECB, the World Bank, the Organisation for Economic Co-operation and Development (OECD), Bank for International Settlements (BIS)-hosted committees and other *fora*. See, for instance, A. Pinna and W. Ruttenberg, 'Distributed ledger technologies in securities post-trading: Revolution or evolution?' ECB Occasional Paper Series, No 172, April 2016; D. He et al., *Virtual Currencies and Beyond: Initial Considerations*, International Monetary Fund (IMF) Staff Discussion Note, SDN/16/03, January 2016 (He et al., 2016); ECB, 'Virtual currency schemes – a further analysis', February 2015 (ECB, 2015); Committee on Payments and Market Infrastructures (CPMI), 'Digital currencies', November 2015; Bank of England, 'Innovations in payment technologies and the emergence of digital currencies', Quarterly Bulletin 2014 Q3; CPMI, 'Non-banks in retail payments', September 2014; The World Bank, 'Innovations in retail payment worldwide', October 2012; Committee on Payment and Settlement Systems (CPSS), 'Innovations in retail payments', May 2012; S. A. Lumpkin, 'Regulatory Issues Related to Financial innovation', *OECD Financial Market Trends*, Vol. 2009 (2).

Accordingly, this paper consists of three parts. Part 1 explores the scope for the wider use of VCs as settlement media for retail payments, as well as the legal issues and questions to which their use would give rise. Part 2 examines the legal implications of the use of distributed ledgers and distributed ledger technologies (DLTs) in the context of the execution and processing of retail payments. Finally, Part 3 provides an account of the core legal issues arising from the use of smart contracts for the processing of payments but, also, other financial transactions that involve an exchange of value.

By way of introduction, it is helpful to briefly explain the meaning of some of the terms and concepts used in this paper, and to define its scope.

As used in this paper, the terms 'FinTech' and 'digital innovation' denote innovations in digital and information technology with an application (actual or potential) to the provision of financial services in general, and retail payment services in particular, and covers DLTs, 'Blockchain', VCs, mobile telephony and other communication technologies accessible to payment service users, new digital advisory and trading systems, and digital innovation- powered peer-to-peer lending and equity crowdfunding platforms. References in this paper to VCs are not intended to cover central bank digital currencies,[5] nor electronic fund transfers but, rather, decentralized, virtual forms of 'money' recorded on a distributed ledger, while references to 'traditional payment rails' are to be understood as references to payment avenues that rely on the intermediation of established financial institutions for the processing of payment instructions and information, and make use of a centralized payment system for the execution and settlement of payments (including instant payments).[6] References to the 'execution' of payments and payment instructions denote the final, unconditional, irrevocable and legally enforceable settlement of payment instructions, understood as the discharge of the payor's payment obligation through the final transfer of funds to the payee. Finally, as used in this paper, the term 'retail payments' denotes low-value payments, typically made outside of the financial markets, that are both initiated *by* and made to individuals and/or non-financial institutions, while the term 'cashless payments' is intended to capture alternatives to cash used for the settlement of fiduciary obligations, and covering both established cash surrogates (such as credit or debit cards) and innovative ones (such as VCs).

5 The reference is to centrally-issued, digital equivalents to *fiat* money, whether complementary thereto or, potentially, issued in substitution thereof, that are not intended as parallel currencies, and which fulfil all three functions of 'money', even if not amounting to new units of account.

6 For reasons of space, instant payments will not be covered in this paper. For a concise account of instant payments and the issues they raise see P. Athanassiou, *Retail instant payments and digital innovation – an overview of risks and challenges*, European System of Central Banks Legal Conference 2016.

2 Innovative media for the settlement of online and remote transactions: the case of virtual currencies

2.1 Conventional settlement media: strengths, weaknesses and scope for innovation

As cash[7] is, historically, the original means of settlement for consumer transactions, a few words are apposite, by way of introduction, on its strengths and weaknesses.

Cash has a number of core advantages over alternative settlement media, and these are mostly linked to its status as *legal tender*, and to its *bearer instrument nature*. *First*, its use results in the *instant discharge* of the underlying fiduciary obligation, without the seller assuming any credit risk, as in the case of non-instant electronic fund transfers or credit-based payments: of all financial transactions, only those settled in cash are 'cleared and settled' instantaneously (many other financial transactions will take several days to clear and settle, even where the entry into the system of a payment order signalling the intiation of their execution, is instant). Linked to this, because physical cash is a bearer instrument, its possession is tantamount to ownership: whoever tenders banknotes or coins is automatically deemed to be their rightful owner. It follows that payees need not conduct any form of 'due diligence' to ascertain the payor's (good) title over cash (although due diligence may be called for, to guard against the risk of counterfeiting). *Second*, cash represents a claim on its issuing central bank, rather than on a commercial bank (as in the case of cash alternatives, such as debit or credit cards): given that central banks are not subject to a default risk, many economic actors will prefer to hold claims on a central bank rather than on any other issuer, such as a commercial bank. Third, physical cash is *anonymous*: in settling their transactions against it, the purchasers of goods or services need not give away private or confidential information, as they would when settling their obligations through the payment system (for instance, by making use of a credit or a debit card); it follows that, where cash is used, there is no risk of personal information being divulged and, potentially, misused, nor is there any transaction record that third parties can access to gauge the payors' payment history or consumer preferences. Finally, the use of cash entails a *censorship-free*, *direct interaction* between the buyer and the seller: the actual *physical* transfer of a banknote entails the transfer of the value it represents, without

[7] The reference is to any physical, non-electronic claim on its issuer (typically, a central bank) in the form of bills or coins – as distinct from credit/debit cards or cheques – that enjoys the status of legal tender or currency in circulation in at least one jurisdiction. Although it only represents a fraction of the total money supply in a modern economy, and despite substantial national variations in terms of the intensity of its use compared to alternatives, cash is over-represented, as a payment medium, in the context of *proximity* retail commercial transactions.

the need for any third party, whether a bank, a broker or another financial intermediary, to 'facilitate', 'sanction' or 'validate' the transfer in question.[8]

But, at the same time, cash is too unwieldy a settlement medium for most E-commerce transactions, which cannot normally be settled in cash, except where so-called 'cash on delivery' schemes are in use.[9] Hence the quest for alternatives. At the time of writing, the five practical alternatives to cash for the settlement of online and/or remote transactions were *account-linked credit and debit cards*, *electronic fund transfers*, *online payment platforms*, *hardware-based digital cash* and VCs. What follows is a basic account of the strengths and weaknesses of the first four of these alternatives, with VCs being explored in some detail in paragraph 2.2.

2.1.1 Account-linked debit and credit cards

Although usage patterns differ significantly across jurisdictions,[10] account-linked debit and, in particular, credit cards, have long been the dominant means for the settlement of long-distance retail transactions. Of the various alternatives to cash, cards were, at the time of writing, the most widely used and, also, the least unconventional.[11] Their core advantage is their broad acceptance, which makes them suitable for long-distance and, *a fortiori*, cross-border retail transactions. But their shortcomings are several. *First*, they can be susceptible to greater or lesser risks of fraud and card-holder data misuse, depending on their authentication technology. *Second*, their use *need not* entail the instant settlement of the underlying fiduciary obligation: to take the example of credit card payments, the payment cycle can take up to three days, from authorization to settlement (especially if the payor does not hold an account with the same bank as the payee merchant), exposing the payee to credit risk in between the initiation of a payment order and the crediting of funds to the payee's account.[12] *Third*, the privilege of card use comes at a cost (mostly in the case of credit cards), in the form of annual subscription fees, interest payments, foreign transaction fees, interchange fees etc. We have left for last what is, perhaps, the most significant shortcoming of account-linked credit and debit cards as payment media: their use pre-supposes the payor's access to the banking

---

8 The opposite is true of electronic fund transfers which, because they are channeled to their recipient through a payment system, with the involvement of one or more financial intermediaries or payment service providers, are subject to higher transaction costs (corresponding to between 2 and 3% of the value of the transfer (M. Bali, 'Les crypto-monnaies, une application des *block chain technologies* à la monnaie', *Revue de Droit Bancaire et Financier* No 2 mars-avril 2016, 14-19, at 14).

9 The market share of cash-on-delivery schemes is relatively static, accounting for around 7%, on average, of payments for all E-commerce transactions (Source: *Worldpay*, 'Global Payments Report 2015', 23).

10 Close to the time of writing, the World Bank found that only slightly over 36% of Germans over the age of 15 used credit cards, as opposed to approximately 57% of Americans and 56% of Australians; substantial variations were also observed in these three jurisdictions in terms of the use of debit cards (The World Bank, The Little Data Book on Financial Inclusion, 2015).

11 According to a recent report, nearly 30% of all payments made in connection with online purchases were settled through credit cards, while another 20% were settled by way of debit cards (Source: *Worldpay*, 'Global Payments Report 2015', 13).

12 It is only a *confirmation* of the payment instructions, and the accompanying payment information, that will be passed instantly from the card issuer's terminal to that of the merchant or service provider. The actual crediting of funds to the recipient's account with the acquiring bank is not, however, instant.

system, rendering them unsuitable for the unbanked. It follows that, despite their merits, account-linked debit and credit cards are not always an ideal means through which to settle long-distance retail transactions.

2.1.2 Electronic fund transfers

Electronic fund (or 'wire') transfers, in the form of either debtor-initiated credit transfers (both on and offline) and creditor-initiated direct debits are preferred methods of payment for online transactions initiated by retail clients or small and medium-sized enterprises that either have no debit or credit card or prefer to, instead, settle their commercial transactions through their bank accounts (presumably for security and/or cost-related reasons).[13]

While no less secure than account-linked debit and credit cards, direct debits are not relevant for all types of E-commerce transactions: their use is mostly limited to low value or recurring payments (i.e. regular, predictable payments, such as subscription fees). Besides, direct debits are error-prone, necessitating customer refunds and chargebacks (to which prescription periods may apply). Moreover, their degree of user-friendliness and the costs that they entail will depend greatly on the manner of their execution (whether online, via an E-banking platform, or offline), as well as on diverging national, banking sector-specific, practices. What is more, neither direct debits nor credit transfers will, as a rule, be settled instantly, meaning that payees take a credit risk on the payor or the payor's bank during the time lag between the authorisation of a payment instruction and the crediting of funds to their account. Finally, both cross-border credit and debit transfers are apt to give rise to complex conflict of laws issues, which would not arise (at least not to the same degree) in the context of cross-border payment transactions settled through other, conventional payment means.[14]

2.1.3 Online payment platforms

Online payment platforms are single operator, account-based schemes, where a single operator offers electronic accounts to registered users, through which to send or receive payments online.

---

13 It follows from a recent study that, in Europe, bank transfers and direct debits are among the preferred payment methods for online use, even where the proprietor has a personal credit card. The examples of iDEAL, in the Netherlands, the SEPA Direct Debit scheme, in Germany, and online banking, in Scandinavia and in some of the Eastern European and Baltic countries, are telling (Source: *Adyen*, 'The Global E-Commerce Payment Guide', Report, 2015).

14 The reference is mainly to the contractual and proprietary aspects of inter-bank payments. While these are not unique to cross-border electronic fund transfers, it is only to an extent that they are addressed by the Rome I Regulation (Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), OJ L 177, 4.7.2008, 6) or the United Nations Commission on International Trade Law ('UNCITRAL'). On the contrary, disputes arising in the context of the use of credit cards for the settlement of cross-border transactions can mostly be resolved by reference to the contracts between the parties to those transactions.

Accounts can be funded through credit cards, debit cards or electronic fund transfers, which users will resort to in order to 'purchase' the electronic value necessary for payments. To make payments, registered users issue electronic payment instructions to the scheme's operator to transfer electronic value from the electronic account they hold with the operator to the payee's electronic account *within the same payment scheme*, without having to disclose their financial details to the payee. It follows that online payment platforms are, effectively, electronic fund transfer service providers. A number of mobile telephony providers also operate similar schemes (in effect, hybrids between payment and remittance-type money transfer schemes),[15] which rely on the use of mobile devices as the means through which to transfer value from the payor to the payee and, in several cases, also as the storage medium for electronic value.[16]

Online payment platforms, of which *PayPal* was, at the time of writing, one of the better known and most widely used examples, present a number of advantages but, also, one or two notable shortcomings, which are not without consequences for their appeal as payment media for online E-commerce transactions. On the one hand, they are readily accessible to a wide range of retail clients, and can be used to effect a wide range of payments; they are more secure compared to debit or credit card payments (as payors need not disclose any of their financial details to the payee merchants); and the transaction costs associated with their use are low (as electronic instructions are processed by the single operator alone, without the involvement of other intermediaries, making these platforms suitable also for the processing of low-value payments). On the other hand, anyone wishing to use the platform, whether to make or to receive payments, *has* to open an account with the single operator, meaning that payments are only possible between scheme participants. Moreover, as these platforms rely on the purchase of electronic value against monetary consideration, account holders take a credit risk on the single operator who, in the event of its insolvency, may be unable to reimburse registered users in respect of the 'real' value converted into 'system' value. Besides, while the payor's account may be debited instantly by the payment platform operator, payment transactions are not executed real-time: the time lag between the debiting of the payor's account and the crediting of funds to the payee's account inevitably gives rise to credit risk, in the event of the single operator's insolvency, even if mitigated by the application of settlement finality rules. Another shortcoming of online payment platforms is that their use postulates the payor's access to the banking system (in common with credit and account-linked debit cards and wire transfers) making them inaccessible to the unbanked.

---

15 The leading examples are *Western Union and MoneyGram*. According to the World Bank, officially recorded remittances to the developing world were estimated at USD 440 billion in 2015, an increase of 0.9% over 2014, the slowest growth rate since the global financial crisis of 2008.

16 Concretely, transfers of value are made by way of encrypted SMS messages sent by payors to their mobile telephony provider, instructing it, as single operator, to transfer value from the payor's account with the single operator, to that of the payee, held within the same scheme.

2.1.4 Digital cash (E-money)

Digital cash (also known as 'E-money') denotes any electronic store of monetary value used for electronic payments to entities other than the digital cash issuer itself, mostly without the involvement of a bank or any other intermediary as settlement agent, hence without the need for access to bank accounts for the execution of the relevant payments.[17] Depending on the technology used to store the monetary value, digital cash will either be hardware or software-based: the focus of this sub-section is on hardware-based digital cash,[18] as server-based variants[19] are the functional equivalents of online payment platforms. Pre-paid payment cards are a typical example of hardware-based digital cash. Hardware-based digital cash is, in essence, a digital representation of – and a secure value-transfer mechanism for – *fiat* currencies, with the technical device in which value is electronically stored effectively serving as a prepaid bearer instrument. Hardware-based E-money presents a number of advantages, common to most digital cash-based products: it is secure,[20] it can be used to make payments outside business hours, and its use leaves a complete trail of all online transactions, enabling E-money users to keep track of their dealings while, at the same time, preserving their anonymity. In some of these respects (but with the notable exception of anonymity), E-money is similar to cash.

However, E-money also has a number of drawbacks. Since it is not legal tender, it is only by way of a *contractual* claim that a consumer or merchant may be able to reclaim the value of their digital currency vis-à-vis its originator/issuer in the event that a digital currency scheme were to be discontinued, or its originator were to become insolvent, or digital cash were to be lost or unlawfully intercepted *en route* to its intended recipient. Digital cash is, therefore, harder to reclaim than physical cash or cash alternatives transferred through conventional payment channels (such as credit cards, where consumers/merchants are immune from loss in the event of fraudulent practices involving the misuse of credit card information), meaning that its use does not, by and large, afford consumers and merchants the same level of protection as the use of cash or credit cards.

What is more, the issuance of digital cash to foreign customers, and its subsequent use as a means of payment for cross-border transactions, may give rise to regulatory, private international law and jurisdictional concerns, as the activity of issuing digital cash (a regulated activity in many jurisdictions) will be subject to the

---

17 For a similar definition see CPSS, *Survey of developments in electronic money and internet and mobile payments*, March 2004, 2.

18 The reference is mostly to card-based E-money, used for small value or for particular types of payment (such as parking or transportation costs, university canteens or sport facilities). Popular card-based E-money schemes include *VisaCash*, *Dumont*, *Mondex* and *Proton*.

19 The reference is to systems allowing for the transfer of electronic value through a telecommunication network or the Internet, with the electronic value itself being stored on the E-money issuer's central server (rather than on a card chip), hence the appellation 'server-based' or 'software-based' E-money. Payments are performed online, and transfers of money are from online accounts, which users can access through the Internet, email or mobile telephone.

20 E-money can be safer compared to cash where a PIN number is required for the completion payment transaction.

laws of the jurisdiction of both the issuer/originator and the customer/user, and to the jurisdiction, *rationae materiae*, of their respective courts.

The foregoing shortcomings significantly limit the attractiveness and usability of E-money, both as a general proposition and, more importantly for our present purposes, as a payment medium for E-commerce transactions, especially where cross-border retail transactions are concerned. They also help explain its limited, domestic-only appeal, at the present time.[21]

2.1.5 Retail payments and their settlement media: what scope for innovation?

As the reader will have gathered from the foregoing discussion, established alternatives to cash present a number of shortcomings compared to cash. More concretely, in terms of *finality*, no form of non-cash payment (with the exception of contactless and instant mobile payments) is as fast as a physical cash payment, both on account of technological constraints but, mostly, for reasons of cost.[22] In terms of *security*, whatever the medium of their settlement, many forms of cashless payments are at a disadvantage compared to cash payments (subject, however, to the risk of counterfeiting), hence the increasing reliance on encryption and data encoding techniques to deliver the necessary level of security. Besides, most forms of cashless payments are at a disadvantage vis-à-vis cash also in terms of *directness* and *anonymity*, as they are settled through the payment system, in the books of a financial intermediary: the use of the payment system for the processing of cashless payments, and the interposition of one or several financial intermediaries for their execution, mean that cashless payments cannot be as disintermediated (i.e. as direct) as a physical over-the-counter cash payment.[23] Ultimately, what most forms of cashless payments have in common is their use of the payment system and bank accounts for the processing of transactions settled in them.

Given that cash, established alternatives to cash and alternative payment schemes currently in use in the context of E-commerce transactions have their shortcomings, there is scope for innovation, whether by way of technological improvements to traditional payment rails or in the form of innovative payment media (or a combination of the two). Although the quest for user-friendly and secure alternatives

---

21 For instance, in the euro area, the aggregated issuance of E-money did not exceed, in December 2015, EUR 7.1 billion, while the value of transactions barely exceeded 73 billion, as compared to EUR 1,427 billion for transactions involving the use of credit cards and 870 billion for transactions involving the use of debit cards (ECB, Payments Statistics, 26 September 2016, available on the ECB's website: www.ecb.europa.eu).

22 Retail payments tend to be settled in batches, for cost-related reasons, in one or several cycles during a business day, generating credit risk during the time lag between the initiation of a payment order and the crediting of the relevant amount to the payee's account.

23 This is not to say that there are no positive sides to intermediated payments, including the customer authentication procedures followed by financial intermediaries active in the execution of payments, and their contribution to precluding unauthorised access to the payment system and/or its use for transfers serving illicit purposes, and to the sharing liability between payment service providers acting on payors' instructions and those receiving payments on behalf of payees. The disintermediated nature of digital technological innovations applied to payments is bound to give rise to legal issues in connection with customer authentication and payment systems security.

to cash is likely to continue fuelling innovation in retail payments, it is only if they were to fulfil certain conditions that innovative payment rails and media are likely to establish themselves in the retail space. Those conditions are as follows: lower or, preferably, no intermediation costs, wide acceptability, irrespective of the type or value of the underlying transaction, instant settlement of the underlying fiduciary obligation, and protection from fraud or misuse.[24]

The remainder of this part will examine the extent to which substitutes for cash, in the form of VCs, are apt to fulfil some (or all) of the above conditions, and what this may spell for their future market prospects.

2.2 VCs and VC networks: definitions, scope and core legal issues

2.2.1 Introductory remarks

Before exploring the legal issues arising from the use of VCs as settlement media for retail payment transactions, a few words are in order, by way of introduction, on our definition of 'virtual currencies'.

Absent a universally accepted definition, 'virtual currencies' can be defined as digital representations of value which, despite not being issued by a central bank or another, comparable public authority, nor being 'attached', subject to certain exceptions,[25] to a *fiat* currency, are voluntarily accepted, by natural or legal persons, as a means of exchange, and which are stored, transferred and traded electronically, without a tangible, real-world representation.[26] This definition of 'virtual currencies' captures decentralised, peer-to-peer[27] VCs – as distinct from E-money or Internet (software)-based payment schemes, which merely facilitate transactions denominated in *fiat* money or in central bank-issued digital currencies – which, while devoid of legal tender status, fulfil, at least to some extent, all three traditional

---

24 For substantially the same views, see G.J.H. Smith, *Bird & Bird, Internet Law and Regulation* (4th edition, Thomson/Sweet & Maxwell, 2007), 874-875.

25 The reference here is to so-called 'settlement coins', denoting VCs with an identifiable issuer. One notable example is the Utility Settlement Coin, promoted by BNY Mellon, Deutsche Bank, Icap, Santander, UBS and Clearmatics. This is an asset-backed digital cash instrument implemented on distributed ledger technology intended to be used for post-trade settlement among financial institutions, which is attached to *fiat* currencies.

26 See the European Banking Authority's (EBA's) Opinion on virtual currencies, 4 July 2014, 11. The Opinion specifies that '[I]t is theoretically conceivable that a central bank or public authority might back a particular [VC] scheme. However, it can be reasonably argued that, in this case, the currency is no longer a virtual but a *fiat* currency'. The ECB had earlier defined VC as 'a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community' (see ECB, *Virtual Currency Schemes*, October 2012, 6). The ECB revisited its definition in 2015 ('a digital representation of value, not issued by a central bank, credit institution or e-money institution, which, in some circumstances, can be used as an alternative to money' – ECB, 2015, 4). On the definition of VCs, also see M. Kalderon et al., 'Distributed Ledgers: A future in Financial Services'? *Journal of International Banking Law and Regulation* (2016) 31(5), p. 243-248, especially 244-246; and D. He et al., 2016, 7.

27 'Peer-to-peer' is to be understood to mean that currency within the network can be transferred from one account to another, without the need for third party intervention.

functions of money[28] by way of *agreement* within their user community.[29] This definition does not, however, extend to centrally-issued digital currencies, such as the central bank digital currencies under consideration, at the time of writing, in several jurisdictions.[30]

VCs, as defined above, are not, at present, the object of harmonised, EU-level regulation (contrary to E-money). That said, several of the EU institutions have, in recent years, taken an interest in VCs, including the ECB, the European Commission, and the European Parliament. VCs are already the subject of some measure of regulation in a number of jurisdictions, including, most notably, the US, Sweden, Japan and Thailand, while international standard-setting bodies, including the CPMI and the International Organization of Securities Commissions (IOSCO), and international financial institutions, such as the IMF, have also engaged with VCs in recent years.

As *bitcoin* is the first and, so far, the most successful example of a virtual currency,[31] a closer examination of its features and technological underpinnings is pertinent.

The term '*bitcoin*' describes both a virtual (crypto) currency (in the form of computer software) and a peer-to-peer payment network, catering for the decentralised[32] proof and transfer of 'ownership' over *bitcoin* units.[33] Thus, *bitcoin* (the currency) and *Bitcoin* (the payment network) straddle the line between a VC and a system for its transfer. *Bitcoin* made its appearance in January 2009, shortly after the collapse of

---

28 The three functions ordinarily attributed to money are to serve as a unit of account, as a medium of exchange and as a store of value (see, for instance, Proctor, 2012, paragraphs 1.07-1. 16, 9-15; and M. Mcleay et al., 'Money in the Modern Economy: An introduction', Bank of England Quarterly Bulletin 2014, Q1. Referring to *bitcoin*, a commentator has expressed reservations as to whether this can serve as either a unit of account or a store of value (D. Yermack, 'Is Bitcoin a Real Currency?' National Bureau of Economic Research (NBER) Working Paper No 19747, December 2013 (Yermack, 2013)).

29 Also see Financial Action Task Force (FATF), 'Virtual Currencies – Key Definitions and Potential AML/CFT Risks', Report, June 2014 (FATF, 2014), 4.

30 The Bank of England was the first to engage with the possible issuance of central bank digital currencies (see J. Barrdear and M. Kumhof, *The macroeconomics of central bank issued digital currencies*, Bank of England Staff Working Paper No 605, July 2016). Sweden's Sveriges Riksbank at one time debated whether to become the first leading central bank to issue a central bank-backed digital currency', 'ekrona' (R. Milne, *Sweden's Riksbank eyes digital currency*, Financial Times, 15 November 2016). The Bank of Canada and the Dutch central bank have also experimented with digital versions of their national currencies, the CAD-coin and the DNBCoin, respectively. For their part, the Bank of Japan, the People's Bank of China and the Central Bank of Russia have also published on the issue or investigated the risks and benefits of issuing some form of central bank digital currency.

31 The success of *bitcoin* is largely attributable to the strong support of its user community, which encouraged traders to adopt it. Other examples, in descending order of market capitalisation, are *Ethereum*, *LiteCoin* and *Ripple*. The technology that underpins them differs, *inter alia* in respect of the protocols through which consensus (i.e. transaction validation) is to be achieved. For an account of the history of earlier virtual currencies, including *Mondex* and *DigiCash*, see S. T. Middlebrook and S. J. Hughes, 'Substitutes for Legal Tender: Lessons from the History of the Regulation of Virtual Currencies' in J. Rothchild, (ed), *Research Handbook on Electronic Commerce Law* (Edward Elgar, 2016) 37-61, at 50-53.

32 The only parties to a *Bitcoin* payment transaction are the funds' sender and the funds' receiver. Whereas a centralized system relies on all parties to trust a third party (the central bank, in most cases) to keep a secure, correct digital record of transactions, *Bitcoin* payment transactions rely on there being numerous copies of this record distributed across the network, rendering the requirement for a trusted third party largely irrelevant.

33 Goldman Sachs Global Investment Research, What is Bitcoin, Issue 21, 11 March 2014, 4; UK Government report: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.

Lehman Brothers and the outbreak of the global financial crisis, and it has since grown to become the world's leading VC, by market capitalisation.[34] A commentator has aptly described *bitcoin* as 'nothing more than a convention established in a distributed algorithm, coordinated securely and reliably by many copies of the same software running throughout the world'.[35] *Bitcoin* are bearer assets, in the sense that a) they are 'unlocked' by computers (nodes) solving complex cryptographic problems and, simultaneously, validating *bitcoin* transactions across the *Bitcoin* network; and b) anyone holding the private key to a *Bitcoin* account is deemed to be their owner.[36]

All copies of the *Bitcoin* ledger match, thereby ensuring the identity of their contents, and guaranteeing the accuracy of the *Bitcoin* ledger as a reliable statement of ownership over each individual *bitcoin*. The very design of *Bitcoin*, and its validation protocol (Blockchain), make it very difficult for 'older' blocks to be rewritten, reversed or altered once a transaction (i.e. a transfer of *bitcoin* units from one account to another) has been validated (i.e. confirmed): it is only by controlling a majority of computational power that individual users could tamper with the state of the ledger, and with the history of the transactions it encapsulates. *Bitcoin's* design ultimately ensures that tokens of value can be securely transferred without the involvement of a trusted third party: instead of trusting in third parties, it is sufficient that *bitcoin* users trust the publicly accessible and secure *Bitcoin* ledger, and the *bitcoin* protocol.

Transferring *bitcoin* involves no more than moving tokens of value from one electronic address to another within the same ledger. Each *bitcoin* is linked, through a public key, to a *Bitcoin* 'account' (effectively, a digital 'wallet'), i.e. to a *Bitcoin* network electronic address, through which to send, receive and store *bitcoin*.[37] A *Bitcoin* account consists of a string of numbers and letters, with no indication of the actual identity of the account holder, who is pseudonymous. Each *Bitcoin* account corresponds to a private key (effectively a code, unique to each account and cryptographically generated at the same time as the account itself), whose knowledge and use are necessary (but also sufficient) for *bitcoin* transfers (i.e. for payments) to be effected from the relevant account.[38] To effect a *bitcoin* transfer (a 'payment') – in other words, to move *bitcoin* from one *Bitcoin* account to another – the payor will use her account's private key to digitally sign a payment message, with details of the amount of *bitcoin* to be transferred, of the payee's address, as well as of the payor's address. The payor will then broadcast this message to the *Bitcoin*

---

[34] At the time of writing, the market capitalisation of *bitcoin* stood at over USD 74 billion, whereas that of *Ether*, the second most popular VC, stood at around USD 35 billion.

[35] S. Bayern, 'Dynamic Common Law and Technological Change: The Classification of Bitcoin', *Washington & Lee Law Review Online* (2014) 2, 22-34 (Bayern, 2014), at 32.

[36] Because assets registered on a ledger are not amenable to possession (by reason of being immaterial), the best proxy to prove possession over them is the holding of the private key, which gives the right to transfer them from one account to another within the network. This point was aptly captured by Jeff Garzik, a *Bitcoin* developer, when he stated that, 'I don't store bitcoins, I store private keys that show I own bitcoins' (E. Rosenfeld, Forget currency, bitcoin's tech is the revolution, CNBC, 14 November 2014).

[37] *Bitcoins* stored in an account can be sourced in one of three ways: either as a reward for serving as a 'miner' (i.e. for allowing the network to use your computational resources – *see infra*); or by purchasing *bitcoins* on a currency exchange); or by selling goods and services against *bitcoins*.

[38] For a concise but comprehensive account of what *bitcoin* is, see D. Quest QC, 'Taking Security over bitcoins and other virtual currency', *Butterworths Journal of International Banking and Financial Law* (2015) 7, 401 (Quest, 2015).

network for verification, with the latter occurring through a process known as 'mining'. 'Miners' (i.e. transaction verifiers running specialised computer software) will inspect *Bitcoin's* public ledger of past transactions to confirm the payor's ownership of the *bitcoin* unit to be transferred, bundle the proposed transfer with other payments and add it, as a new block, to the *Bitcoin* Blockchain, a cumulative record of all individual transactions (blocks) over each individual *bitcoin* unit. Before it can be added to the *Bitcoin* Blockchain, the new block will be cryptographically linked (or 'hashed') to the block that chronologically precedes it, with the hash placed as the header of the proposed block, and becoming the basis for a mathematical puzzle. 'Miners' will compete to solve this puzzle, and the first to do so, as accepted by the majority of anonymous miners who have submitted 'proof-of-work', will be rewarded for their time and effort with a small fee in consideration for their validation services, in the form of newly 'minted' (i.e. unlocked) *bitcoin*.[39] Nodes will then accept the block (i.e. reach a consensus regarding its validity), and add it to a chain stretching back to the very first *Bitcoin* block (the so-called 'genesis block').[40]

As Blockchain – the technological underpinning of both *bitcoin* and the *Bitcoin* network – is the most prominent example of the use of DLTs in a purely financial context, a few words are apposite on Blockchain's design and functionality. Blockchain owes its name to its set-up, which consists of a chain of 'blocks'. Each block represents a digital record of a batch of validated *bitcoin* transactions. To ensure the reliability of the data recorded in the Blockchain, each new block is linked (or 'chained') to its preceding block. Blocks lying outside the chain (so-called 'orphaned blocks') are readily recognizable as they do not refer back to a preceding, validated block. It follows that the key strength of Blockchain is its *transparency*: it is by providing a transparent record of the transactions that it purports to represent, despite the absence of one or more known and trusted intermediaries, that Blockchain has the potential to transform both financial services and the interaction between financial actors, rendering data reconciliations obsolete and 'democratizing' access to the financial system.[41]

While Blockchain is the validation/consensus protocol of the *Bitcoin* network, not all virtual currency networks use the same validation/consensus protocol as *Bitcoin*. For instance, contrary to *Bitcoin*, the *Ripple* payment protocol relies on networks of trusted 'validators' who run *Ripple* nodes and process validations *on behalf of* the *Ripple* network. It follows that, compared to *Bitcoin*, *Ripple* is neither genuinely decentralised nor peer-to-peer, as its definition of trust in the *Ripple* network does

---

[39] This reward (effectively a form of *privatised seigniorage*, devoid of state backing) serves as an economic incentive for 'miners' to run and maintain the *Bitcoin* ledger, rendering *bitcoin* transactions virtually free of charge. The size of the reward has varied over time, with the reward for solving a block halving every four years. By 2140, when the pre-determined ceiling of 21 million *bitcoin* will have been mined, the reward will have been rounded down to zero. One could imagine different Blockchain models, where financial institutions would operate their own Blockchain for financial transactions without such a reward (their reward would be in the form of speed of settlement, cost reduction and enhanced security).

[40] For a definitive description of the bitcoin creation and transfer process see B. Geva, 'Virtual Currencies and Block Chains: Developments and Issues', *National Banking Law Review* (2016) 35(3), 36-42.

[41] A less palatable angle to the immutability of Blockchain is that it makes more difficult the rectification (and, possibly, also the detection) of cases of illicit tampering with the contents of a distributed network.

not require that each node trusts all other nodes (it is sufficient that each node trusts its own, trusted 'validators').[42]

The design of a decentralised payment network's validation/consensus protocol is crucial for the integrity of the payments it processes (and, by extension, for its commercial success).[43] This is hardly surprising, considering that one of the core risks surrounding the use of any virtual form of currency as a means of payment (but which the *bitcoin* Blockchain protocol has overcome) is that of its 'double spending' (see *infra*).[44]

2.2.2 Benefits of VCs

Both VCs and their underlying technologies could, in theory, find practical applications in the field of payments. To the extent that the parties to payment transactions are willing to tender and accept VCs as 'money', these could potentially complement and, in the distant future, possibly compete with, *fiat* money, at least in the retail space. VCs can facilitate the conduct of remote transactions (even if only rarely with immediate finality), they can be conveniently and securely held through any portable device, they are divisible, and their use their holder's pseudonimity.[45] For their part, the technological underpinnings of VCs – whether *Blockchain* or other transaction validation protocols – could facilitate significant future innovation in transaction processing by helping to provide a tamper-free record of payments, and by automating buy-and-sell transactions. By removing middlemen, VCs and their supporting technologies could lead to significant cost gains, including in respect of payments made to merchants,[46] while at the same time lowering the barriers to access to payments, in the form of fees or currency exchange charges imposed by banks, credit card networks and online payment platforms. The parties to payment transactions (and, especially, those devoid of, or with only limited access to, banking

---

42 *Ripple's* quorum-like transaction validation protocol is fundamentally different from *Bitcoin's* proof-of-work blockchain protocol: the former delivers transaction validation at a fraction of the time required by *Bitcoin*, but there are trade-offs in terms of the consistency across ledgers that the *Ripple* protocol can achieve. For a detailed account of *Ripple's* consensus algorithm, see M. T. Rosner and A. Kang, 'Understanding and Regulating Twenty-First Century Payment Systems: The Ripple Case Study', *Michigan Law Review* (2016) 114(4), 649-681; D. Schwartz et al., 'The Ripple Protocol Consensus Algorithm', Ripple Labs Inc., 2014.

43 To take the example of the *Bitcoin* network, the digital proof it offers of the chronological order of transactions entered into its ledger need not necessarily offer the requisite and/or most practical safeguards against the risk of double spending. Without such safeguards, there can be no legal certainty in the use of VCs for the making of payments, whether retail or other.

44 The issue of double spending was drawn attention to by *bitcoin's* presumed inventor, who proposed the *bitcoin* protocol precisely in order to overcome that problem (see S. Nakamoto, 'Bitcoin: A peer-to-peer electronic cash system', November 2008).

45 A. Milne, 'Cryptocurrencies from an Austrian Perspective', April 17, 2017, 7-8.

46 This is not to say that the acceptance by traders of VCs would not come at a certain cost. The volatility risk alone would translate into costs, which would help explain why *bitcoin* service providers enter into agreements with retailers, under the terms of which payments received in *bitcoin* are to immediately be converted back into *fiat* currency, so as to mitigate the *bitcoin* exchange risk for retailers.

services, such as the recipients of remittances) will benefit from lower transaction costs for payments and fund transfers, and from lower access-to-payment costs.[47]

For all their promises, VCs and their underlying technologies also carry certain risks, legal and non-legal alike. We will focus, below, on the core legal risks, acknowledging from the outset that the non-legal risks of VCs can also be substantial.[48]

2.2.3 VCs: core legal issues

The use of VCs as payment media in the context of long-distance, retail E-commerce transactions would give rise to a number of legal issues, mostly linked to the *decentralisation* of the networks where VCs are created, and of the ledgers where transactions over them are recorded. These are presented, below, in no particular order of priority.

One of the core challenges to be overcome in the context of VCs is that of avoiding the risk of their 'double-spending'. Modern, centralized payment systems address this concern through master ledgers, maintained by trusted third parties for the processing of third party payments, and recording the flow of money across the various accounts within the payment system by tracking, in a reliable manner, adjustments in the balances of those accounts. As decentralised networks recording transactions in virtual money lack both trusted third parties and master ledgers, it is only if their validation protocols are reliable, sufficiently robust *and* practical to use that there can be trust in VCs, and in the payments they facilitate.[49]

Related to the above, decentralised networks recording transactions in VCs can be susceptible to system-wide fraud if their process of achieving 'consensus' within the network of users (in respect of the creation and 'putting in circulation' of VCs) is poorly designed or prone to tampering. The validation protocol of *Bitcoin* is designed so that prospective fraudsters would require control of a majority (i.e. 51%) of the total computing power across the entire network so as to be able to tamper with the decentralised digital ledgers where the creation and transfer of transactions in VCs are recorded. Policy makers may wish to reflect on how to avert the risk of co-ordinated pools of 'miners' or 'nodes' (or, possibly, third parties) mustering the degree

---

47 That said, unlike centralised (retail) payment systems that can operate at relatively low marginal costs because of economies of scale in information-processing, decentralised networks relying on numerous 'miners' or 'nodes' to process, in parallel, the same transactions risk, foregoing the efficiency of centralised transactions-processing. Thus, decentralised payment systems can only compete with centralised transfer systems on cost if their transaction-processing set-ups can be rationalised. In this regard, see also A. Robleh et al, 'Innovations in payment technologies and the emergence of digital currencies', Bank of England Quarterly Bulletin 2014, Q3.

48 Non-legal risks include VC volatility, which can expose currency holders to losses should their VC holdings depreciate in value, and technology dependence, as VCs are contingent on their underlying technology to reliably record their storage, spending, and exchange.

49 Even so, if payments in VCs were to pick up, it is conceivable that double-spending would need to be recognized by legal systems across the globe as a criminal offence.

of computing power necessary to fraudulently alter the contents of decentralised ledgers, with an impact on the integrity of payments performed in VCs.[50]

Other sources of legal risk for the users of VCs are bound up with *legal uncertainties* surrounding their status as 'money', their issuance and the finality of transactions settled in VCs. Unlike centrally issued *fiat* currencies, VCs will typically lack an issuing authority, whose law would govern their issuance and legal attributes. The practical question arising in this context is that of the possibility (or otherwise)[51] of applying the *lex monetae* principle to a payment, or any other, commercial transaction settled against delivery of a VC. Under the *lex monetae* principle, when a monetary obligation is expressed in a particular currency, the parties to it are imputed with a choice of the law of the jurisdiction of the currency's issuance to determine what that currency means, and to which particular jurisdiction the obligations it gives rise to fall under. Without clarity on a VC's *lex monetae*, to legally define the VC in which an obligation is expressed, the parties to a transaction settled against it would not be in a position to safely predict the consequences on their obligations of a change in the VC's definition, nor, *a fortiori*, the impact of its eventual demise on those obligations.

VCs also raise questions of relevance to *whether and how they fit into the existing legal and regulatory framework*. To take the example of VC networks, one of several pertinent questions is whether these would qualify as payment service providers, within the meaning of the Payment Services Directive II (PSD II).[52] The latter differentiates among credit institutions, E-money institutions and, more importantly for our purposes, 'payment institutions', defined as 'legal person[s] … granted authorisation … to provide and execute payment services throughout the Community.'[53] Similarly, it is not entirely clear whether the exchange of goods against VCs could qualify as a 'payment transaction', within the meaning of PSD II[54] or whether a VC network, such as *Bitcoin*, would fall within the scope of the definition of 'payment system'.[55] To take another example, that of the EU's harmonised Anti-Money Laundering/Counter Terrorist Financing (AML/CTF) framework, AMLD IV does not treat VC exchanges as 'financial institutions' subject to the anti-money laundering and counter terrorist financing requirements set out in it.[56] Question

50 The creator of *Bitcoin* readily acknowledged that the robustness of the network was conditional on the majority of computing power within it being controlled by nodes that are not co-operating to attack the network (Nakamoto, 2008, 1).

51 Admittedly, to postulate that the *lex monetae* principle may apply to VCs is to accept that these are currencies. As explained in this paper, there is no consensus around this point (indeed, the weight of scholarly opinion and jurisprudence would seem to suggest that the opposite is true).

52 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 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, OJ L 337, 23.12.2015, 35.

53 PSD II, Article 4(4).

54 PSD II defines payment transactions as 'act[s] initiated by the payer or on his behalf or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee' (Article 4(5)). 'Funds' within the meaning of the PSD II are 'banknotes and coins, scriptural money or electronic money' (Article 4(25)).

55 Pursuant to Article 4(7) of PSD II a payment system is a 'funds transfer system with formal and standardised arrangements and common rules for the processing, clearing and/or settlement of payment transactions.'

56 AMLD IV, Article 3(2). This is contrary to the EBA's Opinion on virtual currencies (see footnote 27).

marks also surround the subjection of virtual currency networks to the Markets in Financial Instruments Directive (MiFID),[57] which, at the time of writing, only applied to investment firms and credit institutions.[58]

VCs (and the networks catering for their transfer) also raise *regulatory competence* issues, in terms of determining which jurisdiction (or jurisdictions) can claim the competence to regulate dealings in VCs, whether as payment instruments or, possibly, as commodities. Given their global reach, it appears likely that more than one jurisdiction would have an interest in and a claim over the regulation of the circulation and use of VCs. This is because, as mentioned above, the components of a decentralised VC network would, presumably, be located in more than one jurisdiction, with VCs themselves existing within a digital universe, at the same time within and outside the reach of any particular jurisdiction. In terms of the actual *subject matter* of potential regulation, a number of areas appear relevant, for instance, whether dealing with VCs could trigger a licensing requirement, and whether *trading* in VCs – as commodities, rather than as money – could give rise to regulatory/licensing implications for those engaging in the purchase and sale of virtual against sovereign currencies.

The *anonymity* of VC networks, other than *Bitcoin*, is also bound to generate legal as well as regulatory concerns. Decentralised payment systems can be designed to be more anonymous compared to credit card processing systems or online payment platforms, even if they need not necessarily match the level of anonymity of cash. To take the example of *Bitcoin*, *bitcoin* accounts are pseudonymous, while the *bitcoin* protocol does not require the identification of its actual users.[59] As mentioned earlier, *Bitcoin* has no central server, no central oversight body and no AML software to monitor and identify suspicious transactions. As a result, there is no central location (no 'administrator', so to speak) to serve as the focal point for an investigation or a seizure of assets.[60] Similarly, the global reach of VCs, and the fact that VC networks can be accessed through Internet-enabled mobile phones increase the potential of their use to sidestep AML/CTF safeguards when making cross-border payments or fund transfers.[61]

We have left for last a question that is bound to exercise the minds of lawyers and lawmakers alike: that of the *fundamental legal characterisation* of VCs, whether as *property rights*, or as (public) *money* or as another *sui generis* type of asset. We explore this question below.

---

57 Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments amending Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC of the European Parliament and of the Council and repealing Council Directive 93/22/EEC, OJ L 145, 30.4.2004, 1.

58 MiFID, Article 1.

59 *Bitcoin* users are not guaranteed the same level of anonymity as the holders of cash. It is, in theory, possible for transactions to be 'tied' together based on the entries in *Bitcoin's* distributed ledger and, then, linked to the actual user's identity. Similarly, users who wish to convert *bitcoins* into *fiat* money can be identified as the currency exchange systems are expected to enforce the applicable regulations on customer identity and AML/CTF.

60 Authorities could target individual exchangers for client information they may collect.

61 FATF, 2014, 9-10.

2.2.3.1 VCs as money or currency

At the time of writing, both national legal doctrine and case law were divided on whether VCs qualify as 'money'[62] or 'currency'[63] as opposed to being commodities or another type of proprietary asset. At a basic level, it can be argued that, to the extent that a VC operates as a medium of exchange for those willing to accept it, as a store of value, and as a unit of account, it is apt to qualify as 'money', at least in conceptual and functional terms. The above would, no doubt, hold true of *bitcoin*, which was *ab initio* designed for use as money and has, indeed, been so used since its very inception.[64] What is also undisputed is that VCs have value (despite their volatility), meaning that they can also be the object of money laundering, in the same way as public money or currencies. The obvious counterargument is that, because they lack a) a central authority to define and implement a *policy* geared towards safeguarding their stability, b) a national legislator eager to attribute to them the coveted status of legal tender, and c) a physical existence, VCs are not 'currencies'.[65] Differences of opinion in terms of the characterisation of VCs are unsurprising, considering their novelty but, also, the elusive nature of the very concept of 'money', notwithstanding its ubiquity and practical relevance to everyday commercial dealings. The competing theories of money expounded in the literature hint at the difficulty of reaching a consensus on the question of the precise status of VCs.[66] To illustrate the differences of opinion in terms of whether VCs, in general, and *bitcoin*, in particular, qualify as 'money' or 'currency', we examine, below, some of the relevant case law in the EU and the US.

In a ruling delivered in October 2015, in the matter of a tax dispute (on whether VAT was payable on the purchase and sale of units of *bitcoin*), the Court of Justice of the European Union (CJEU) confirmed that *bitcoin* is a 'means of payment and that it is accepted for that purpose by certain operators';[67] accordingly, transactions relevant to the exchange of *bitcoin* against traditional currency and vice versa were exempt

---

62 The consensus is that in order for an object to qualify as money, it should possess the characteristics of a store of value, a medium of exchange, and a unit of account. On the definition of money, see A. B. Abel, and B. S. Bernanke, *Macroeconomics* (5th edition, Pearson, 2005), 266-269.

63 We use the terms 'money' and 'currency' as synonyms, despite the fact that they do not fully overlap: while all currency is money, not all money is currency (there is a territorial dimension to the concept of 'currency', which the concept of 'money' lacks).

64 S. A. Wiseman, 'Property or Currency? The Tax Dilemma Behind Bitcoin', *Utah Law Review* (2016) 2, 417-440, especially 418 and 439.

65 It is a distinct question whether VCs could nonetheless qualify as 'money', a concept that is broader than 'currency'. See B. Geva, 'Disintermediating electronic payments: digital cash and virtual currencies', *Journal of International Banking Law and Regulation* (2016) 31(12), 661-674, where it is stated that, 'with neither physical existence nor official status, virtual currencies are neither 'currency' nor 'legal tender'; however, the author goes on to state that the above is not necessarily fatal to the characterisation of VCs as money, given that they can serve as media of payment or exchange that could affect the stability of prices, impact the financial system and generate payment system risks.

66 For an account of the concept of money, and the three main competing theories of money, see Proctor, 2012, 5-63; and C. Bamford, *Principles of International Financial Law* (OUP, 2011), 7-40. For an application of those theories to VCs, see J. Perkins and J. Enwezor, 'The legal aspects of virtual currencies', *Butterworths Journal of International Banking and Financial Law* (2016), 569-572, especially 570-571.

67 Case C-264/14, *Skatteverket v David Hedqvist*, paragraph 52. This author's reading of the ruling is that, in the eyes of the CJEU, *bitcoins* (and, presumably, other VCs) do qualify as money, since one of the key attributes of 'money' (an elusive concept, by all accounts, at least legally) is that it serves as a medium of exchange in commercial transactions.

from VAT under the provisions of the VAT Directive[68] concerning transactions relating to 'currency, bank notes and coins used as legal tender'.[69] The ruling of the CJEU is consistent with the treatment of *bitcoin* as 'money/currency', since the utility of any chattel as a medium of exchange largely determines its characterisation as money. The CJEU's ruling is at odds with an earlier decision of a civil court in the Netherlands,[70] in a case involving an imperfect *bitcoin* sale and purchase transaction. The buyer had sought to purchase an amount of *bitcoin* units, and paid for their corresponding value in euros; the seller only delivered a fraction of the agreed *bitcoin* units, prompting the buyer to sue the seller. Ruling in favour of the buyer, the Court ordered the seller to pay back to the buyer the *original* value of the undelivered *bitcoin* units, together with interest and legal costs, but declined to award damages for lost profits, claimed on the basis of the substantial appreciation in value of *bitcoin* between the time of the conclusion of the sale and purchase agreement and the court ruling. The Court stated that *bitcoin* is neither 'legal tender' ('*wettig betaalmiddel*') nor 'current money' ('*gangbaar geld*') within the meaning of Book 6 of the Dutch Civil Code,[71] nor E-money, within the meaning of the Financial Supervision Act. However, it could be viewed as a medium of exchange between individuals, such as gold, and it could, therefore, be acceptable as a form of payment in the Netherlands. The Court's ruling is neither entirely consistent with the status of bitcoin as a commodity (in which case the Court would have, presumably, entertained the buyer's claim for lost profits), nor with that of its treatment as 'money/currency'; it is, however, consistent with the treatment of *bitcoin* as a medium of exchange, in which property rights can subsist.

The picture is no less fragmented across the Atlantic. In July 2016, a Florida Circuit Court ruled that, for the purposes of Florida criminal law, *bitcoin* was property but *not* money or currency, due to its limited acceptability by traders, the substantial fluctuations in its value, and the decentralized nature of its network, which was not backed by a central reserve or any other central authority, nor by anything of value.[72] Contrary to the ruling of the Florida Circuit Court in *State of Florida* v *Espinoza*, a US District Court judge in New York ruled in *United States* v *Murgio* that *bitcoin* met the definition of money,[73] rejecting the defendant's plea to dismiss criminal charges brought against him for his involvement in the operation of *Coin.mx*, an unlicensed *bitcoin* exchange.[74] Much the same conclusion had been reached earlier by a US District Court in Texas in *SEC* v *Shavers*,[75] where the founder and operator of an

---

68 Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax, OJ L 347, 11.12.2006, 1.

69 Ibid., Article 135(1)(e).

70 Case C/08/140456/HA ZA 13-25 *Rechtsbank Overijssell* (May 14, 2014).

71 According to Article 112 of the Code, '[m]oney paid to perform an obligation must, at the time of payment, be current in the country in whose currency payment is made.'

72 *State of Florida v Espinoza*, Case No F14-2923 (Fla. 11th Cir., 22 July 2016) ('[T]hey [*bitcoin*] are certainly not tangible wealth and cannot be hidden under a mattress like cash and gold bars').

73 'Bitcoins are funds within the plain meaning of that term' … 'Bitcoins can be accepted as a payment for goods and services or bought directly from an exchange with a bank account. They therefore function as pecuniary resources and are used as a medium of exchange and a means of payment.'

74 *US v Murgio et al*, US District Court, Southern District of New York, No 15-cr-00769, 28 September 2016.

75 *Securities and Exchange Commission v Trendon T. Shavers and Bitcoin Savings and Trust*, Civil Action No 4:13-CV-416, 2013 US Dist.

online *bitcoin* investment fund, accused by the Securities Exchange Commission (SEC) of operating an illegal Ponzi scheme, questioned the jurisdiction of the Court over the matter, under the Securities Act 1933, arguing that *bitcoin* was not money and, as a consequence, did not fall within the remit of the SEC nor within the scope of US securities law.[76] Rejecting the arguments, the Court found that it did have jurisdiction, as *bitcoin* 'can be used as money' and possesses the attributes of a 'currency or form of money', despite limitations in terms of its breadth of acceptance. Similarly, in *United States* v *Faiella*,[77] US District Court Judge Jed S. Rakoff denied a motion brought by the defendant, an unlicensed *bitcoin* transmitter, to dismiss a pending money laundering action against him, premised on the assertion that *bitcoin* is not 'money' under federal law; in the Court's view, '[B]itcoin clearly qualifies as "money" or "funds"' as *bitcoin* could be 'easily purchased in exchange for ordinary currency, acts as a denominator of value, and is used to conduct financial transactions.' The legal status of *bitcoin* was at stake in proceedings before the US Bankruptcy Court for the Northern District of California in February 2016, in the context of a dispute between a *bitcoin* mining company and an individual, hired in 2013 to promote the company's products (the 'promoter'), and paid for his services in *bitcoin* units.[78] There, the bankruptcy judge ruled that 'bitcoin are not United States dollars', but reserved judgment on the question of whether the trustee's recovery could be limited to the value of the *bitcoin* units at the time of their transfer to the promoter or should encompass their subsequent appreciated value. While not settling the debate in terms of the status of *bitcoin* as a currency or a commodity, the Court's ruling is consistent with its treatment as a form of property.

Whether or not *bitcoin* qualifies as 'money' or 'currency', the one common thread running through the case law on either side of the Atlantic is that *bitcoin* is a *de facto* medium of exchange, to which value (and, by implication, also a certain measure of legal protection) attaches. Ultimately, the extent to which a particular VC will qualify as 'money' will depend on its individual features, on the extent to which these are conducive to its acceptability as a means of payment, as well as on its distinct regulatory treatment: the question of its status is not, in other words, one that lends itself to an abstract answer. What *can* be said, as a general proposition, is that a) modern currencies exist in the context of sovereign states;[79] b) *de lege lata*, none of the VCs in use at the time of writing was backed by a sovereign issuer or a central

---

76 The 1933 Act defines the term security to include an 'investment contract', which, under the so-called *Howey* test (SEC v W.J. Howey Co., (328 US 293), 1946) is any contract, transaction or scheme involving 'an investment in money'.

77 39 F.Supp.3d 544 (Southern District of New York, 2014).

78 *In re Hashfast Technologies LLC v Lowe*, No 15-3011DM Case No 15-03011 (Northern District California, 19 Feb 2016).

79 The euro is not an exception to this rule: far from being a 'currency without a sovereign', the euro is backed by the 19 Member States of the EU that had, at the time of writing, chosen to pool their sovereignty in matters of monetary policy and adopt the euro as their single (national) currency.

bank; and c) VCs appear to fulfil, even if only to varying degrees, all three functions of money.[80]

2.2.3.2 VCs as property rights

Several of the world's legal systems regard tokens of value as 'property',[81] helping to explain the emerging consensus that VCs relying on the use of tokens may evidence property rights[82] (or may be compatible with the law of property). As no *in abstracto* analysis of the treatment of VCs as property rights is possible, suffice it to make, here, some general remarks.

It could be argued that holding a *bitcoin* or another VC through a VC exchange is not conceptually dissimilar to holding a conventional form of currency through a depositary financial intermediary, and that VCs are '*a form of intangible private property, a valuable digital artefact … an asset and … the valuable property of their current owner, who can transfer them as and when she pleases*'.[83] Nevertheless, three *caveats* require expression.

The first is that, unlike the holders of conventional currencies, the holders of VCs created on un-permissioned networks do not typically have a claim against an identifiable legal person as *issuer*: their claim (to the extent that there is one) would be against the distributed, peer-to-peer network in which a VC has been generated, and through which it can be exchanged. However, even this form of recourse would risk proving illusionary, absent an identifiable legal person against which redress could be sought in the event of grievances arising from the operation of an un-permissioned VC network.

The second is that with (most) VCs there is neither a physical nor, *stricto sensu*, a digital object that property rights could readily be exercised over: as explained earlier, transfers of ownership over VC units involve no more than a change in a shared ledger entry, instigated by the holder of a private key to a VC account. The implication of the foregoing is that a classic property law analysis of VCs is far from straightforward, as the specificity and enforceability of property rights, and the protection they benefit from against interference with their peaceful enjoyment, are among the hallmarks of property rights.

The third is that, with VCs, there is no immediate association between a *Bitcoin* account and an identifiable account owner, who remains pseudonymous: as property

---

80 We do not share the Yermack's view that *bitcoin* only serves the medium of exchange function of money. The very existence of *bitcoin* exchanges suggests that *bitcoin* can serve as a store of value (despite its volatility, which is not a privilege of *bitcoin*), and as a unit of account, as it is possible to use *bitcoins* to value most economic items, including the cost of goods, services, assets, liabilities, income, and expenses (see Yermack, 2013).

81 D. Fox, *Property Rights in Money* (OUP, 2008), paragraph 1.140.

82 There is scholarly support for the proposition that, for the purposes of civil jurisdiction, VCs should be treated as tangible property (M. I. Raskin, 'Realm of the Bitcoin: Bitcoin and Civil Procedure', *Fordham Journal of Corporate and Financial Law* (2015) 20, 969-1011).

83 R. Bollen, 'The Legal Status of Online Currencies: Are Bitcoins the Future?' *Journal of Banking and Finance Law and Practice*, (2013) 24, 272-293, at 279.

law is about the relationship between (identifiable) people and things, and the ability of the holder of property rights to enforce those rights, one may wonder whether *bitcoin* could meaningfully be the subject matter of proprietary rights.

At the same time, it is undisputed that the holders of VCs have an *expectation* that their holdings will be protected as (intangible) property: even if it cannot decide the question of the classification of VCs as 'property' rights, the legal value of this expectation is far from negligible and could, in and of itself, provide the basis for the legal protection of *bitcoin* holdings, against theft or another form of unlawful interference. A case in point is the UK High Court ruling in *Armstrong DLW GmbH v Winnington Networks Ltd*[84] where, unbeknown to the defendant, the claimant's password to its online 'carbon credits' account was hacked, facilitating the unauthorised transfer of its contents to the defendant's account, and its eventual sale. The claimant had no claim in tort (for conversion), given the intangible nature of the misappropriated carbon credits, nor was there a contract it could rely on to recover those credits or their value. However, the High Court ruled that the claimant had a common law proprietary claim over the carbon credits which, while intangible, qualified as property, and was, accordingly, entitled to a money award. What the High Court ruling suggests is that, even in jurisdictions where the distinction between tangible and intangible forms of property is deeply ingrained, there could be remedies on the basis of which to protect the interests of the holders of forms of intangible property, including VCs, against unlawful interferences with their enjoyment. That said, to accommodate the specificities of VCs, and to square the circle of their treatment as repositories of 'rights', normative adjustments would appear advisable, especially if the use of VCs were to become more widespread. It is difficult to accept, not least for reasons of public policy, that *de facto* tokens of value, freely transferable, convertible into conventional currencies, and routinely used as means of payment or as objects of investment, would not benefit from the protection typically afforded to other objects of value, whether as property or as contractual or as another form of 'right' (be it known to the law or novel).

As the public acceptance of VCs as a form of payment increases, so does the urgency of the quest for clarity as to the proprerty law status of VCs. For, the legal implications of treating VCs as 'property', rather than as mere representations of value in which no property rights subsist, as currency or as mere private law (contractual) rights, are manifold: national law protection of property (including intellectual property) rights,[85] such as the property torts of conversion or trespass, assignment and perfection-related requirements (including where a creditor wishes to take a VC as collateral, by perfecting a security interest in it), criminal offences (including theft and fraud), and tax liability (in the form of capital gains tax), would

[84] [2012] EWHC 10 (Ch), 11 January 2012.

[85] As they are software/computer codes, VCs could be the object of intellectual property protection, in particular copyright, as 'literary works'. For copyright to subsist in a work, this has to meet an originality threshold. In the case of *bitcoin*, it appears that their code is no more than a variant of the previous one (with the only element of differentiation residing in the segment of code that records the unique signature corresponding to each transaction). It may thus be that *bitcoin*, as a computer code, would not satisfy the 'originality' requirement. Moreover, it is difficult to pinpoint any specific entity as the author of the computer code of each *bitcoin* code given that it is the self-executing peer-to-peer *Bitcoin* network that causes the string of code to change with each transaction.

only apply or attach to VCs if these were to qualify as 'property', under national law. The proprietary nature (or otherwise) of VCs will also determine the extent to which they can become encumbered by a security interest, as well as the application (or otherwise) to them of the *nemo dat quod non habet* rule in the context of commercial transactions involving VCs.

2.2.3.3 VCs as contractual rights

Even if VCs were neither money/currencies nor property, they could still qualify as *contractual* rights.

To take the example of *bitcoin*, what an investor has 'is simply a contract right against the operator of the website …' and, '[T]his sort of right is meaningfully different from having possession of personal property', as it is subject to a risk of default of the 'website', while it is also not 'identical, economically or legally, to possession', as it has to be 'fought, won and enforced …'.[86] While it is true that ownership of a *bitcoin* or any other VC gives one the right to use, sell and make contracts over them,[87] a contract law analysis of *bitcoin* or other VCs would risk proving problematic, unless a VC has an identifiable issuer. Referring to *bitcoin*, it has been aptly suggested that, 'one does not have to agree to abide by any terms of use or otherwise agree to take or refrain from taking any action to acquire ownership of a bitcoin' and that, '[L]ikewise, the other participants in the system are not bound by any contract express or implied'.[88] Similarly, it has been argued that, 'ownership of a bitcoin does not confer a legal right against the participants in the Bitcoin system'.[89]

In light of the above, it is difficult to see how the holding of a *bitcoin* can establish any manner of (enforceable) contractual right between its holder and the peer-to-peer network where *bitcoin* is created and traded, or between its holder and the participants to that framework, given the open source nature of the *Bitcoin* software, and the absence of an identifiable issuer against which the holder could bring a contractual claim premised on her *bitcoin* holdings.

---

86 Bayern, 2014, 25-26.

87 R. Grinberg, 'Bitcoin: An Innovative Alternative Digital Currency', *Hastings Science & Technology Law Journal* (2012) 4(1), 159-208, at 199.

88 Straus et al., 2015, 186.

89 Bayern, 2014, 31.

3 Distributed ledgers and their underlying technologies: application to payments, strengths, weaknesses and core legal issues

3.1 Introduction

Electronic transactions processed through traditional payment channels are settled *centrally*, i.e. *through the payment system*, in the books of a financial intermediary (typically a bank) or a non-bank payment service provider with access to an established financial intermediary, mostly through a bank account. The most widely used payment option, across traditional payment systems, is the 'slow', low-cost payment option, requiring payment system participants to submit their payment instructions to the system operator, for clearing, netting and, finally, settlement. The clearing and settlement of *international* payments – which involves an intricate web of (correspondent) bank and non-bank intermediaries – is notoriously 'slow, inconvenient, [and] costly',[90] with the latency of the settlement cycle between the issuance, by a payor, of a payment instruction and the crediting of the payee's account giving rise to liquidity and credit risks.

Depending on the speed of their in-built consensus (i.e. transaction validation) process, payment solutions/protocols similar to those currently in use in connection with VCs are apt to lead to the instant (or near instant) point-to-point settlement of payment transactions,[91] while also reducing operational costs associated with reconciling exceptions and failures. It follows that the rationale underlying the operation of decentralised *networks* for the transfer of VCs could, if applied to retail payment systems, reduce delays in the execution of payments,[92] dispense with 'central points of failure', promote payment network resilience and security and, *in extremis*, do away with the very need to clear payment transactions between the owners of settlement assets native to the same distributed ledger.

This part provides an account of the use of distributed ledgers and DLTs in the context of the execution and processing of retail payments, followed by a non-exhaustive, summary account of some of the core legal issues that their use would pose for the initiation, clearing and final settlement of retail payment instructions.

---

90 Federal Reserve System, *Strategies for Improving the US Payment System* 2015, 25 No 35. In this regard, also see CPMI, *Correspondent Banking*, July 2016.

91 Whereas *Bitcoin* transactions usually take several minutes until validation and at least one hour (or more) before they are considered final, the *Ripple* network transfers value within seconds, i.e. in real-time. The difference in speed is attributable to the less time and energy-consuming consensus (i.e. validation) process of the *Ripple* protocol, compared to *Bitcoin's* heavier validation (proof-of-work) process.

92 In particular, funds could be credited instantly to the payee's account, if both the payor and the payee held accounts (and funds) within the same ledger, without the need for recourse to intermediaries, and without the delays (and costs) that their involvement entails.

3.2 Significance of centralised ledgers for the operation of the modern financial system

A 'ledger' is a 'book or other collection of financial accounts'.[93] Ledgers are a familiar concept in banking and finance. Before the age of digitalization, ledgers existed *physically*, to provide a true and original record of all movements in and out of the accounts that bankers made available to their customers. The modern financial system is built around a network of *electronic* ledgers (the present-day equivalent of the 'bankers' books' of previous centuries), maintained by interconnected financial institutions and financial market infrastructures, from central banks and commercial banks (acting as liquidity providers, payment service providers or custodians) to CSDs, clearing houses and central counterparties. These ledgers are synchronised by robust but costly (and fallible) reconciliation and financial-control processes. The recording of transactions among identifiable, regulated counterparties, and the 'management' – i.e. the constant updating – of ledgers are among the very *raisons d'être* of modern financial market infrastructures, including payment systems, CSDs and clearing houses.

To illustrate the utility of ledgers, we take the example of a simple transfer of funds between parties A (the payor) and B (the payee). A transfer of funds will typically involve the banks of the payor, the payee, potentially other banks (for instance, correspondent banks, if the fund transfer is to take place cross-border) and, ultimately, one or more central banks. Each of these entities will maintain its own ledger to record payment transactions, by crediting one account and debiting another. When money, in the form of a deposit balance reflecting a depositor's redeemable claim against her bank, moves through the payment system, from A to B, A's deposit balance with her bank is decreased, while that of B is increased, through a process of 'settlement', which involves their respective banks updating their ledgers to adjust A's and B's new deposit balances. Commercial banks will hold balances with their central bank, while end-customers will hold balances with commercial banks, acting as intermediaries: it is by holding deposits from each commercial bank involved in a payment transaction, and by adjusting, in its 'master' ledger, the balances of those deposits, so as to reflect transfers of funds, that the apex institution can settle obligations between commercial banks and their customers. Commercial banks will, in turn, maintain their own ledgers, to ensure the accurate reconciliation and recording of their transactions, and those of their customers.[94]

By credibly recording fund transfers (or changes in ownership over financial assets, including those created and existing digitally), and by facilitating the settlement of the mutual obligations of counterparties to payments or other financial transactions, centralised ledgers are the final guarantors of trust in the entire financial system. It is,

---

93 See Oxford online English Dictionary definition of ledger.

94 Reconciliation among the parties to a transaction may either occur as part of each transaction's clearing and settlement process (i.e. on a transaction by transaction basis) or as part of the daily balancing activities. In this regard see CPSS/BIS, *The Role of Central Bank Money in Payment Systems* August 2003, 1-2; and M. Haentjens and P. de Gioia-Carabellese, *European Banking and Financial Law* (Routledge, 2015), Chapter 9, 155-168.

ultimately, for reasons of systemic stability that the modern financial system relies on identifiable, trusted participants to act as 'gatekeepers', and to provide identity-matching and management services for the benefit of the prospective end-users of financial services.

The preceding account demonstrates the challenges inherent in the substitution of centralised by decentralised ledgers for the recording of payment transactions, and the massive shift that this would entail in terms of the transition from a centrally controlled to a peer-to-peer model for the execution and processing of payments.

3.3 DLTs: definition and types

'DLTs' denote the *corpus* of information and data-sharing technologies through which computers ('nodes') participating in a 'peer-to-peer' computer network can *validate* and *record*, chronologically and securely, *asset transfers* (such as payments of money or transfers of book-entry securities), *changes in state* (i.e. changes in the ownership of assets), *balances* of funds or securities, or combinations of (some of) the above. Thus, 'DLTs' encompass all of those technologies the aim of which is to facilitate the connection of manifold nodes within a network to a shared database (a 'distributed ledger') destined to provide a transaction validation and consensus record.[95]

Our definition of DLTs hints at their core promise, and their revolutionary potential in a payments context. As explained above, at present, core payments are *centralised*: the competent central bank will typically sit at the apex of the payment system, acting as central 'clearing bank' (or central 'settlement institution'). The process of payment data-validation and reconciliation across the multi-tiered payment system is time-consuming (not least because some of the necessary validations and reconciliations are conducted *manually*) but, most of all, labour-intensive, costly, and prone to errors;[96] at the same time, however, it is a process that allows for multi-level checks, prescriptions and corrections, and guarantees a higher probability of compliance with legal and regulatory prescriptions. DLTs promise to change the intermediated and tiered structure of modern financial market infrastructures, and to eliminate labour-intensive, manual reconciliation processes in legacy multilateral platforms, by enabling financial market participants (such as parties to payments or securities transactions) to keep track of transactions or adjustments of balances or changes in the ownership of assets (including cash balances and securities holdings) in a distributed ledger, updated real-time, with every new transaction; the state of the ledger is to be deemed authoritative, despite the absence of a trusted third party i.e. a financial intermediary with overall responsibility for the processing of transactions in the relevant payment, securities clearing and settlement or other multilateral system. It is because of their potential to revolutionise financial markets

[95] See J. Kvarnström and A. Gustafsson, 'Blockchain: From Why to What and Regulating How' *International In-House Counsel Journal* (2016) 9(36), 1-7, at 1.

[96] According to Santander Bank, DLTs could help banks save up to USD 20 billion a year in cross-border payments-related infrastructure costs and, also, in securities trading and compliance (see Santander InnoVentures et al., *The Fintech 2.0 Paper: Rebooting Financial Services* 2015, 15).

by changing their intermediated architecture and centralised management, validation and reconciliation set-ups, that DLTs have captured the attention of policy makers and financial market participants alike. Ultimately, DLTs hold the, arguably, spectacular promise of substituting commercial trust in intermediaries with trust in digital, distributed technology and computer code.[97]

A few words are in order on the different types of DLTs. Our discussion, above, should not lead the reader to the conclusion that distributed ledgers should, perforce, be *fully* decentralised. It is possible to distinguish between four main types of distributed ledgers: 'unrestricted' (or 'open'), 'restricted' (or 'closed'), 'public' and 'private'.[98] Unrestricted ledgers are those that are open to anyone with the technical ability to participate in them (i.e. to operate a node), whereas restricted ledgers are those whose participants are selected on the basis of pre-defined criteria. Unrestricted ledgers are colloquially referred to as 'un-permissioned' (or 'permission-less'), since every one of their participants is free to contribute data to them, without a single controlling entity to act as transaction validator or network administrator, whereas restricted ledgers are colloquially referred to as 'permissioned', since their participants are subject to restrictions in terms of the activities they are authorized to undertake (whether to update the ledger, or to validate its state, or to issue new assets in it, or to enforce the regulatory, contractual and service rules subject to which the ledger operates). Public ledgers differ from private ones in terms of access rights to their audit trail: anyone may access data recorded in a public ledger, whereas data recorded in a private ledger may only be read and updated by its participants (or a sub-set thereof) or designated third parties (such as regulators or overseers).

There are obvious trade-offs to the different levels of decentralisation referred to above: fully decentralized, un-permissioned ledgers are inherently less efficient, as shared computing among the participants of a peer-to-peer network may require synchronization, adding to costs[99] and generating demand for increased data-storage capacity.[100] Cost and data-storage considerations aside, it is conceivable that only some of the less decentralised variants could be deemed desirable for use in a financial services environment, especially where offline assets are concerned,[101] for reasons of system integrity, legal and regulatory compliance, and data confidentiality. Similarly, the idea of a risk management framework through which to modify ledger entries in the event of unauthorized or unintended transactions, or to initiate reverse transactions, is easier to reconcile with the concept of a *permissioned*

---

97 Blockchain has aptly been referred to as a 'machine for creating trust' (The Economist, *The Trust Machine*, 31 October 2015).

98 These concepts are, needless to say, *not* mutually exclusive: unrestricted ledgers are, perforce, public, while restricted ones may be either private or public.

99 The less decentralised a network is, the less costly its validation process: the number of messages to be exchanged amongst network participants before transactions can be verified has a knock-on effect on system capacity, latency and, ultimately, cost. Lower network resilience is the flipside of a low-latency/low-cost system: the more restricted the pool of data validators, the greater the risk of system failures.

100 Data storage and network band-width are likely to generate concerns should decentralized nodes seek to substitute high-powered centralized processing centres in their computation and data storage tasks.

101 The reference is to assets that are not 'native' to a ledger but exist, legally, outside the relevant ledger, such as *fiat* money or securities issued and held in a real-world CSD.

ledger than it is with that of an *un-permissioned* one (without prejudice to the technical possibility of offsetting entries to reverse such transactions). At the same time, unlike un-permissioned variants, permissioned ledgers would require governance arrangements, to determine how a small group of participants is to exercise control over the ledger, and what their liability will be vis-à-vis ledger users.

3.4 Legal issues

Given that distributed ledgers can record balances of funds, as well as transfers of value from one account to another (whether of money or securities) the clearing and settlement of payments is likely to be among the financial sector activities to be impacted the most by the eventual adoption of DLTs. We explore, below, the main areas of legal concern relevant to the use of DLTs for the holding of funds, and for the execution of payment transactions.

3.4.1 Legal status of transactions performed in a DLT environment

In DLT adoption scenario, the validity and enforceability of payments performed in a DLT environment will be an obvious area of legal concern. In particular, clarity would be desirable, in such a scenario, on the *legal effects* of entries in a distributed ledger recording the transfer of funds across 'accounts': such transfers may either give rise to an actual transfer of ownership over the underlying assets, or only have a presumptive (rather than a constitutive) legal effect or, merely, trigger a contractual obligation to transfer funds upon fulfilment of whatever formalities may apply under national law(s) for their valid transfer.

3.4.2 Settlement finality in a DLT environment

The validity and enforceability of transfer orders and fund transfers performed on a distributed ledger will, *inter alia*, depend on whether the latter can achieve settlement finality, as one of the key attributes of contemporary, centralized payment systems. It is only if there is clarity as to whether and when settlement finality can be attained in a DLT environment that DLTs can offer the legal certainty guarantees to which the parties to payment transactions aspire.[102]

Depending on the specificities of their design,[103] DLT-based networks may not achieve settlement finality in the *legal* sense of the term (i.e. as systems): this is

[102] It has been observed that, 'the industry will be looking for legal certainty relating to the status of transactions on a DLT before they are recorded on a Securities Settlement System recognised under the Settlement Finality Directive (for transactions settled in the EU)' (London Stock Exchange Group, *Response to ESMA discussion paper on 'The Distributed Ledger Technology Applied to Securities Markets'*, September 2016, 2). It is submitted that similar considerations would apply to payment systems.

[103] To take the example of the *Bitcoin* network, miners are under no enforceable obligation to execute a transaction, which they could even decide to block, impacting on the network's legal and practical ability to achieve finality of transfers.

because the *technical* finality of transfer orders processed in a DLT environment need not match the commonly-shared *legal* understanding of the concept of finality.[104] Besides, it is not clear whether the currently applicable statutory settlement finality safeguards would apply to decentralized multilateral platforms, to the extent that these may not legally qualify as 'designated systems', within the meaning of the Settlement Finality Directive (SFD)[105] or any other equivalent legal framework, nor is it clear which entity is to guarantee the finality of transactions if, as in the case of a fully disintermediated platform, there were to be no identifiable entity to operate the platform, unlike in the case of conventional securities settlement or payment systems, where a CSD or another system participant will assume responsibility for the irrevocability of the transactions processed through it.[106]

The finality properties of different, digital innovation-facilitated payment or securities trading architectures would need to be thoroughly explored and understood, with decentralized ledgers used for the processing of transfer orders either brought within the scope of the national settlement finality rules or being taken as a reference point for changes to these rules, to ensure that those transfer orders enjoy the same level of finality as those settled within centralized systems.[107] If neither of the above can be achieved, it is not clear that there is a case for the use of distributed ledgers for the settlement of transfers of value.

3.4.3 Conflict of laws

One of the more appealing aspects of DLTs is that they can facilitate cross-border transactions through the simultaneous location of DLT network-participating nodes in more than one jurisdiction. What this entails, by necessary implication, is that payment transactions taking place in a DLT environment would, potentially, fall within the legal and regulatory remit of every jurisdiction where a DLT network node exists. Thus, a pertinent legal question is *which* law or laws govern payment or other financial transactions processed in a DLT environment and, related to this, which court could rightfully assert *ad personam* jurisdiction over a dispute arising from, or in

---

104 Finality of transactions processed in distributed ledger environments is *probabilistic only* (rather than deterministic, as in the case of centralised ledgers), giving rise to warranted concerns in terms of title transfer (also see J. A. Garay et al., 'The Bitcoin Backbone Protocol: Analysis and Applications', 7 March 2017, 4-5; and R. Sams, 'Bitcoin Blockchain for Distributed Clearing: A Critical Assessment', *The Capco Institute Journal of Financial Transformation* (2015) 4, 39-46, at 44).

105 Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems, OJ L 166, 11.6.1998, 45. For an account of the notion of finality and the main features of the SFD see M. Vereecken, 'Directive 98/26/EC on the European Union Payment Systems and Securities Settlement Systems', in *Settlement Finality in the European Union: The EU Directive and Its Implementation in Selected Jurisdictions*, M. Vereecken and A. Nijenhuis (eds), (Kluwer Legal Publishers, Deventer, 2003), 13-75.

106 Referring to FinTech-driven platforms, it has aptly been observed that, '[B]ecause they lack central administrators by definition, blockchain-based systems are unforgiving: there is no helpdesk to reset a lost password, say. Bank bosses may be tempted to stick with the slower, pricier systems they know' (Blockchain − The next big thing, The Economist, 9 May 2015).

107 Drawing on the April 2012 CPSS-IOSCO Principles for financial market infrastructures, it could be argued that finality need only be a concern in the context of systemically significant ledgers. However, given the interlinkages between shared ledgers, including non-systemically important ones, and other, systemically significant financial market infrastructures, such as payment systems, and the attendant risk of contagion, a restriction of the scope of finality to systemically significant ledgers only would not appear advisable, for policy reasons.

connection with, the processing of such transactions.[108] The urgency of providing an answer to the above questions would be compounded by the absence, in a DLT environment, of a single account or register where funds are held and, as a consequence, by the lack of a clear connecting factor between them and a given jurisdiction.[109]

3.4.4 Insolvency proceedings

For the reasons explained in the preceding paragraph, the application of insolvency rules to DLT platforms and VC exchanges is likely to represent something of a challenge.

To illustrate the point we take the example of the European Insolvency Regulation (EIR),[110] under the terms of which, for debtors falling within its scope of application,[111] the 'main insolvency proceedings' are to be opened in the Member State where the debtor has the centre of its main interests.[112] The EIR further states that, 'the law applicable to insolvency proceedings and their effects shall be that of the Member State within the territory of which such proceedings are opened'.[113]

The implication of the foregoing is that ownership rights over assets stored on a distributed network (for instance, in an E-wallet) would be determined, upon insolvency, by reference to the law of the competent insolvency court. However, it may be difficult to *a priori* determine the law of the debtor's 'centre of main interests', where the debtor in question is a decentralised DLT platform. This difficulty is bound to create uncertainty in terms of the insolvency treatment of the assets stored in such platforms, including in terms of the applicable transactional avoidance rules.

3.4.5 Compliance with legal and regulatory requirements

DLTs would not change the requirement for entities involved in the provision of payments or other regulated services to comply with the applicable regulatory requirements, including AML/CTF, know-your-customer (KYC), sanctions and tax-related legal requirements: the market integrity, financial stability and fiscal policy

---

[108] Disputes could, for instance, arise in the event of a fraudulent or erroneous transaction: as the locus of the relevant 'act' may be impossible to ascertain, courts in every single jurisdiction where a DLT network node is located could simultaneously claim jurisdiction over the dispute.

[109] In terms of conflict of laws, the most appropriate solution for securities held with an intermediary would presumably be to identify the 'place of the relevant intermediary' by determining the branch where the securities account is maintained. However, where there is no intermediary and no branch, as in the context of certain types of DLTs (in particular un-permissioned ones), identifying a concrete connecting factor to a specific jurisdiction will be challenging.

[110] Regulation (EU) 2015/848 of the European Parliament and of the Council of 20 May 2015 on insolvency proceedings, OJ L 141, 5.6.2015, 19.

[111] This is defined in Article 1(2) to exclude insurance undertakings, credit institutions, investment firms and collective investment undertakings, within the meaning of EU law, leading the author to the conclusion that the EIR would, a priori, apply to DLT platforms, to the extent that these are possessed of legal personality.

[112] Ibid., Article 3(1).

[113] Ibid., Article 7(1).

considerations that underpin those requirements remain valid, whatever the precise technological underpinning for the provision of regulated financial services. They would, however, raise concerns in terms of identifying the 'entity' that is to become subject to regulatory compliance, at least in the case of unrestricted networks.

Traditional intermediaries, with an emphasis on credit institutions, money transmitters and brokers, are under a duty to apply KYC checks, to monitor transactions and to report suspicious dealings to their national financial intelligence units or other competent authorities (in this regard, see the provisions of the AMLD IV, in the EU). If distributed ledgers were to become more firmly established, policy makers and regulators would need to consider how existing regulatory requirements would apply to new ways of clearing and settling value transfers, whether adjustments are necessary to those requirements to bring new actors within their scope,[114] and how regulatory requirements, existing or new, are to be enforced, especially in the case of unrestricted networks. This is without prejudice to the obvious potential of DLTs to facilitate data sharing, including the sharing of data relevant to the monitoring of money laundering and terrorist financing, and to reduce the costs associated with compliance with the applicable AML/CTF framework.

3.4.6 Protection of transactional and other data in a DLT environment

At a basic level, DLTs are no more than data-exchange and data-sharing tools, for the processing and storage of transactional and other data, including private data. In a financial services context, the efficient sharing of data is crucial, for market participants and supervisors alike. However, the protection of data confidentiality is no less crucial than its efficient sharing, especially where the underlying data is of a proprietary nature.

One of the defining features of DLTs is that the transactions they process and record rely on a chain of records, which cannot be deleted. Moreover, once recorded in a distributed ledger, information is to, in principle, remain stored in it *ad infinitum*. On a different note, the transaction-level transparency of un-permissioned distributed ledgers,[115] and their accessibility to anyone equipped with the appropriate software and Internet access, can make them ideal targets for malicious third party attacks.

How is data confidentiality and the 'right to be forgotten'[116] to be ensured in a DLT environment, especially where there is no central point of reference to assume

---

[114] D. Mills et al., 'Distributed ledger technology in payments, clearing and settlement', Finance and Economics Discussion Series 2016-095, Board of Governors of the Federal Reserve System, (Mills et al., 2016), 30.

[115] While distributed ledgers offer asset ownership-level transparency (which would be desirable for reasons of settlement finality, and for the monitoring of the validity of title transfers) they also offer transaction-level transparency (which is, in principle, undesirable given the proprietary nature of the underlying information).

[116] Under the EU General Data Protection Regulation, due to come into force in Spring 2018, the private data of EU subjects is to be protected and used only for legitimate data processing purposes; moreover, EU subjects are to have a 'right to be forgotten' by any data processor and may demand the deletion of their private data. These obligations are to apply to all data processors irrespective of their location, as long as they process the personal data of EU subjects.

responsibility for protecting data confidentiality, and how are shared ledgers to be shielded from external attacks without their participants having to disclose their digital identity to a central entity, so that malicious actors can be identified and prosecuted?

As decentralized ledgers may, depending on their design, disclose more information compared to their centralized peers, data confidentiality concerns are bound to feature prominently in their context.[117] In particular, while disintermediation in the form of a multiplicity of ledgers replicating the same content can, in theory, bring with it enhanced IT safety and system resilience benefits,[118] these benefits may, depending on their design, come at a price, in the form of loss of confidentiality and privacy: transactions taking place in an un-permissioned DLT network are visible to every single network participant. If data confidentiality and privacy cannot be protected, it is unlikely that there would be demand for the wide-scale deployment of ledgers (especially fully un-permissioned ones) in a financial sector context.

The achievement of DLT network resilience against external attacks raises less of a dilemma but no less serious concerns. DLTs are, in theory, less vulnerable to outside attacks compared to centralized ledgers, both on account of their use of cryptography and because the accuracy of their contents does not turn on the reliability of a single set of records but is, instead, a function of the contents of an entire disintermediated network of identical ledgers, which cannot, except in the most unusual of circumstances, be tampered with across the board. Otherwise put, to be successful in a shared ledger environment, it is not sufficient for malicious attackers to only infiltrate one user: instead, they would need to attack multiple copies of the shared record held at the level of the relevant peer-to-peer network.

In truth, the protection of un-permissioned distributed ledgers against external attacks is no less of a *technical* than it is a *legal* matter, and its pertinence is not limited to DLT platforms. That said, legal certainty and stability considerations would strongly militate in favour of the introduction of regulatory safeguards to protect, also in a DLT environment, proprietary interests against third party attacks, acknowledging that the same level of protection should apply to all financial sector databases, whether or not these rely, for their use, on DLTs.

The legal complexities alluded to above are compounded by regulatory issues of relevance to data storage and reporting, areas of particular legal notoriety and country-specificity. Laws and regulations protecting privacy (for natural and legal persons alike) and data confidentiality may restrict data storage and retrieval across national borders. This looks set to be an issue in a fully un-permissioned DLT environment handling international transaction flows, where every transaction is to be distributed, for validation purposes, across the entire network of nodes.

---

[117] In this regard, see Astri, Whitepaper on Distributed Ledger Technology, 11 November 2016, 55.

[118] Multiple ledgers replicating the same content are, a priori, safer compared to single master ledgers (notwithstanding the fact that the latter are backed-up).

4 Smart contracts: challenges and opportunities

As explained in more detail in this part, smart contracts are computer codes that allow agreements to execute themselves once certain real world conditions have been met. The processing of electronic payments could be one of several financial sector-specific applications of smart contracts. Indeed, any payment transaction the triggering of which turns on an ascertainable event could be pre-programmed and automated through smart contracts. The use of smart contracts to pre-programme and automate payments could facilitate their execution but, for the reasons explained below, it could also render error detection and remediation a challenging task, while at the same time raising a number of purely legal concerns, linked to the automaticity, irreversibility and decentralisation of smart contracts.

We explain, in this part, the core legal issues arising from the use of smart contracts for the processing of payments. Our analysis, below, is also valid for other financial transactions involving an exchange of value.

4.1 Smart contracts: working definition

As a prelude to our examination of the benefits of smart contracts, and of the legal issues to which their use would *a priori* give rise, we consider, in this section, their *definition*, and chart their core financial sector-specific use cases.

It is often the case that the debate on DLTs, and their potential applications to financial services, involves *some* mention of 'smart contracts'. What this debate lacks is a commonly accepted understanding of the underlying concept: indeed, there are as many definitions of smart contracts as there are commentators, with the differences amongst the proposed definitions pointing to subtle but, often, legally

significant differences of perception with regard to the smart contracts phenomenon.[119]

Given the lack of a settled, commonly accepted definition of smart contracts, we would propose defining them as 'contractual-type' arrangements embedded in software, which the latter can validate, execute and record *automatically*, on a DLT platform, as soon as certain pre-programmed conditions, agreed upon by human agents, have been met, based on information fed into the DLT itself or received from a pre-defined (mostly external) source. From a functional standpoint, what distinguishes a smart contract from a conventional one is the potential it has, on account of the software in which it is embedded, to automate pre-agreed responses, conditional on the occurrence of specific events, determined *ex ante* by the contractual parties, and to update records accordingly, once those events have materialised. Our definition, above, is without prejudice to whether smart contracts will necessarily amount to *legally binding* arrangements, a question to which we revert later in this paper.

The 'canonical real-life example' and 'primitive ancestor' of a smart contract is the 'humble vending machine',[120] which automates the execution of *irrevocable* transactions by dispensing items in return for money. Vending machines only dispense items once the pre-agreed conditions (consisiting in the payment of a predetermined amount) have been fulfilled. Those who, wishing to purchase an item, are willing to tender the necessary amount of money can enter into a contract with the machine, which is to act as 'contract bearer'. Since both the items for sale and the money received in return for them are securely retained within the vending machine, the latter can protect both against external 'attacks'.

The most notable practical example, to date, of the convergence between DLTs and smart contracts is the decentralised platform operated by the *Ethereum Foundation*,

---

[119] Szabo, who is credited with devising the concept of smart contracts, has defined smart contracts as 'a computerized transaction protocol that executes the terms of a contract', adding that '[T]he general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries' (see N. Szabo, The idea of smart contracts, 1997). Pinna and Ruttenberg have defined smart contracts as 'a way of transposing the contractual obligations imposed on users into the digital distributed ledger' (A. Pinna and W. Ruttenberg, 'Distributed ledger technologies in securities post-trading: Revolution or evolution?' ECB Occasional Paper Series, No 172/April 2016, 18). Mills et al. have perceived 'smart contracts' as the transposition, in a DLT environment, of conditional contractual obligations, to ensure the automatic execution and recording, within a shared ledger, of predefined actions as soon as a pre-agreed event or events have occurred (Mills et al., 2016, 14). More recently, Lauslahti et al., have defined smart contracts as 'digital programs based on a Blockchain consensus architecture that automatically implement their internal logic as certain preconditions are met, and which are also able to prevent unauthorised changes of their internal logic …' (K. Lauslahti et al., 'Smart Contracts – How will Blockchain Technology Affect Contractual Practices?' ETLA Reports No 68, 9 January 2017 (Lauslahti et al., 2017), while Koulu has defined smart contracts as 'programmable contractual tools, … contracts embedded in software code' (R. Koulu, 'Blockchains and Online Dispute Resolution: Smart Contracts as an Alternative to Enforcement', SCRIPTed (2016) 13(1), May 2016, 40-69, at 53 (Koulu, 2016)). IOSCO has, for its part, defined smart contracts as '… computer programs written on the distributed ledger. These computer programs are pre-written logic stored in, and executed by the nodes in the DLT. Upon the execution and verification of the actions triggered by the smart contract, the latest state (outcome) associated with the business activities will be recorded and stored in the block' (IOSCO, 51-52).

[120] N. Szabo, 1997.

a Swiss non-profit organisation, crowdfunded in 2014.[121] In common with *Bitcoin*, *Ethereum* is a distributed network composed of thousands of nodes running the *Ethereum* Blockchain-type software. However, unlike *Bitcoin*, which exists to record, in its distributed ledger, the creation and transfer of *bitcoin*, *Ethereum* not only records the creation and transfer of *Ether* (its native VC, the first ever with in-built, general-purpose smart contract execution capability) but, also, runs smart contract applications on a customised Blockchain, serving as a shared global infrastructure that can simultaneously represent ownership in assets, and which platform participants (nodes) can use to 'create' markets, store logs of debts or promises, and move funds or other value in accordance with pre-determined instructions, free of human intermediation. Although inspired by *Bitcoin*, *Ethereum* marks, through its smart contract capabilities, a shift from *Bitcoin's* functionally limited scope, allowing agreements to be written in code and to be executed automatically through its network of participants.

4.2 Benefits of DLT-enabled smart contracts

Smart contracts, within the meaning of our proposed definition, have been possible for as long as computers have existed. What is genuinely new about DLT-enabled smart contracts is the programmable use that they make of DLTs and Blockchain, and the benefits that their programmability could come with for financial market actors, in terms of *certainty of execution of contractual agreements*, *immutability/ censorship resistance* and *cost-savings*. We briefly examine, below, the core benefits of DLT-enabled smart contracts.

As explained earlier in this paper, distributed ledgers are, in principle, more secure and less error-prone compared to conventional, centralized ledgers, on account of their shared nature, and the fact that, in their case, there is no need for data reconciliations. In a Blockchain or in other DLT environment, automated (or automatable) contracts for the transfer of value could provide contracting parties with a greater degree of certainty in terms of the performance of their pre-determined contractual obligations, in accordance with the terms stored in their software. In the same way that they can ensure the validity of ledger updates, DLTs can also cater for the faithful execution of smart contracts, free from external tampering, generating an environment of commercial trust, in which perfect strangers can trade with one another without the need for a trusted intermediary or another comparable gatekeeper to assume responsibility for contract execution.

The substitution of trust in intermediaries with trust in computer code, as part of the contract-creation process, is not the only benefit that DLT-run smart contracts would have to offer. The automated nature of DLT-powered smart contracts could narrow down (or altogether eliminate) the scope for human error (except in the design of the computer code itself), while at the same time being conducive to the formation of contracts that are virtually unbreakable. Equally importantly, the automated nature of

[121] For an account of the Ethereum Blockchain-based platform, see V. Buterin, 'A Next-Generation Smart Contract and Decentralized Application Platform, Ethereum', White Paper, 2013.

smart contracts could drastically remove the costs (and the inconvenience) inherent in the exchange of paper-based contractual documentation, while at the same time facilitating the process of the execution of contractual transactions.

Despite their promises, smart contracts also raise a number of legal challenges and practical questions, addressed in more detail later in this part.

4.3 Legal nature of smart contracts

By emulating the logic of contractual agreements, smart contracts hold the promise of *complementing* or, even, *displacing* conventional contracts. Is this to say that smart contracts qualify, legally, as contracts in their own right, and could be the source of rights and obligations for the parties to them? This core question is examined in the remainder of this section.

4.3.1 Introductory remarks

It has been argued that the term ‘smart contract’ is a double misnomer: the arrangements brought under their umbrella are neither 'smart' nor binding, in the strict legal sense of the term.[122] Indeed, it can be argued that, to the extent that what triggers the formation, execution and recording of a smart contract is the fulfilment of a pre-agreed and pre-programmed condition or the occurrence of a contractually relevant, ascertainable event, rather than a genuinely autonomous, own-initiative ‘decision’ of the software in which a smart contract is embedded, the latter cannot meaningfully be termed ‘smart’. Moreover, to the extent that certain smart contracts exist to implement other, *existing* contracts (rather than mere framework agreements) they cannot *stricto sensu* qualify as contracts in their own right but, rather, as settlement mechanisms or follow-up, accessory arrangements, the function of which is to merely implement prior contractual agreements or, alternatively, to serve as mere evidence of a contract, the full terms of which may or may not be ascertainable on their basis. The legal implication of the preceding observations is that smart contracts would only be legally binding on their parties if their execution were to in no way contradict a prior contractual arrangement between the parties nor any mandatory, public law provisions applicable thereto at the time of their ‘formation’, and if their terms were complete and ascertainable on the basis of their software. What this, in turn, entails, is that computer code will not invariably be ‘law’, and that the software in which a smart contract is embedded cannot (or may not always) be the source of legally binding obligations. How warranted are the above conclusions?

Three introductory observations are in order, before we attempt to provide the elements of an answer. A *first* observation is that the moniker ‘smart contract’ need not be conclusive in terms of the legal characteristics of the underlying phenomenon:

[122] C. Lim et al., ‘Smart Contracts: Bridging the Gap Between Expectation and Reality’, 11 July 2016, Oxford Business Law Blog (Lim et al., 2016).

the appropriate frame of reference is that of national contract law, as interpreted and applied by domestic courts, rather than the nomenclature opted for by those who write or support of smart contracts. A *second*, related observation is that much will turn on the features of a particular smart contract (which may incorporate, by reference, the terms of another, conventional contract), as well as on national law prescriptions in the jurisdiction where the question arises:[123] smart contracts will differ from one another, and the same is true of national contract law, which need not accommodate them. Our final observation is that, despite the challenges it poses, the question of the legal status of smart contracts merits an answer − even if, for the reasons explained here, this can only be a general one − given the seminal role that contracts and contract law play in the organization of economic relations in contemporary societies: whatever the appetite for innovation, and however malleable or adaptable contract law may be,[124] there is bound to be a measure of skepticism vis-à-vis innovations that purport to improve on or, *a fortiori*, to altogether dispense with the need for conventional contracts and, by implication, with the legal safeguards and protections that contracts provide for the benefit of their parties.

4.3.2 Smart contracts and the 'Code is law' doctrine

In the wake of the Internet Revolution, it was argued that computer code operates *outside* the legal framework, and that 'Code is law',[125] in the sense that computer code provides the normative underpinning of cyberspace, which conventional legal frameworks cannot meaningfully hope to regulate. Applied to smart contracts (a phenomenon that had yet to manifest itself at the time when the 'Code is law' thesis was propounded), the foregoing doctrine would postulate that whenever computer code is implemented through a network of computers running on a decentralised platform, it is the computer code alone that carries any legal weight, as the code in question 'resides nowhere and everywhere.'[126]

In spite of its common sense attraction, the 'Code is law' doctrine places the very concept of smart contracts under stress, for several reasons. The first reason is that it misrepresents the limitations of computer code and, in particular, the degree of difficulty inherent in transposing *legal* into *technical* rules: simple, unambiguous legal rules may well lend themselves to encoding, but the same need not be true of more complex, less straightforward ones, the application of which may involve an element of interpretation, discretion or appreciation, rendering the task of their

---

123 For an account of the main parameters of an answer to this question, in a number of leading jurisdictions, see R3/N. R. Fulbright, *Can smart contracts be legally binding contracts?*, White Paper, 2016 (Fulbright, 2016).

124 See E. Mik, 'Formation Online', in M. Furmstrom and G. J. Tolhurst, Contract Formation: law and practice (OUP, 2010), 159.

125 '… [i]n cyberspace, we must understand how code regulates … *Code is law*' (L. Lessig, *Code and other laws of the cyberspace* (Basic Books, 1999), 89). Another scholar had earlier referred to this incipient body of rules as 'Lex Informatica' (J. I. Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules Through Technology', *Texas Law Review Volume* (1998) 76(3), 553-593).

126 P. Vigna and M. Casey, The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order (St. Martin's Press, 2015), 66.

implementation into code something of a challenge.[127] The second reason is that it glosses over the continuing relevance of external legal rules in the regulation of human behaviour in cyberspace: despite the libertarian exuberance inspired by the advent of the Internet,[128] traditional legal concepts of property, contract and criminal law continue to play a dominant role in the regulation of the online activities of human agents in cyberspace,[129] and they are likely to continue doing so for the foreseeable future, refuting the thesis that cyberspace operates in a legal vacuum. A *third* reason (and, perhaps, the most powerful objection to the application to smart contracts of the 'Code is law' doctrine) is the following: to accept that the 'Code is law' is to *ipso facto* accept that the parties to an automated contract are to invariably be bound by the consequences of its digital execution, courtesy of its computer code, without a possibility of judicial review, even where the computer code has 'malfunctioned', whether on account of a bug or due to an original technical design fault, or because it has been hacked into by intruders or malicious users, or where it has otherwise led to manifestly unintended results, not foreseen by the parties to a commercial transaction at the time of the drawing up of the computer code, that are contrary to their interests. Code correctness is, in other words, something that the 'Code is law' doctrine merely *postulates*. In this regard, the precedent of the 'attack' on *The DAO* is highly instructive.

The DAO was launched on the *Ethereum* Blockchain as a crowdfunding and capital management platform, intended to operate *without* a fund manager. *The DAO* was to allocate funds (in the form of *Ether*) collected from its users (its investor-members) to third party projects, in line with the wishes of its investor-members, similar to a venture capital fund. The voting rights of the users of *The DAO* (which reflected the amount of *Ether* that users had pledged in exchange for tokens) were governed by its computer code, with 'curators' (permissioned users) selecting projects for funding and putting them up for a vote.[130] On 17 June 2016, an unknown user exploited a loophole/weakness in the computer code of *The DAO* to drain from it an estimated 3.6 million of *Ether* (or one third of the net worth of *The DAO*, at the relevant time), which he channelled into a 'child DAO', for a project he had proposed. Some members of *The DAO* argued in favour of a 'hard fork' (effectively, a change in *Ethereum's* protocol), so as to reverse transactions in each block, and refund the misdirected *Ether*; other users opposed this solution, as it would contradict *Ethereum's* credentials as an immutable record of past transactions, and violate the

---

127 'Yet, the practice of transposing legal rules into technical rules is not an easy task. As opposed to legal rules, written as general rules in a natural language that is inherently ambiguous, technical rules can only be implemented into code, and thus necessarily rely on formal algorithms and mathematical models. Regulation by code is therefore always more specific and less flexible than the legal provisions it purports to implement' (P. de Filippi and S. Hassan, 'Blockchain technology as a regulatory technology: From code is law to law is code', (2016) First Monday (21), 12 (Filippi and Hassan, 2016)).

128 J. P. Barlow, 'A declaration of the independence of cyberspace', 1996.

129 The adoption of entire rafts of legislation, on both sides of the Atlantic but, also, globally, at around the time when the Internet went mainstream (such as, for instance, the E-Commerce Directive in the EU (Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L 178, 17.7.2000, 1), the Digital Millennium Copyright Act in the US, and the Anti-Counterfeiting Trade Agreement) testify to the predominant role of the law in regulating human activities carried out through the use of modern communication technologies.

130 Mills et al., 2016, 29.

irreversibility of its code.[131] Was the 'attack' on *The DAO* a hacking incident or was it, instead, an illustration of a programming feature of a computer code producing effects that were at odds with the contracting parties' intentions?

Far from implementing the presumed contractual agreement binding together the users of *The DAO*, its software may have openly *contradicted* that agreement. Interestingly, the contract between *Slock.it*, the entity behind *The DAO*, and its user community stated that,

'[A]lthough the word "contract" is used in The DAO's code, the term is a programming convention and is not being used as a legal term of art. The term is a programming convention, not a representation that the code is in and of itself a legally binding and enforceable contract. If you have questions about legal enforceability, consult with legal counsel.'

The above statement suggests, on the one hand, that the smart contracts built into *The DAO* were never intended to qualify as binding contracts in their own right, to the extent that they were unsupported by conventional contractual documentation between the parties, allowing their genuine intentions to be surmised; and, on the other hand, that, if in doubt, it was the law of contract, and any conventional contractual documentation between the parties, that was to prevail over the computer code. While the foregoing, case-specific conclusion need not be decisive as to the connotation attaching to the term 'contract', as applied to *other* smart contracts, it does question the extent to which smart contracts are to always be perceived as stand-alone agreements, in the context of which computer code is the only arbiter of the agreement it represents or, instead, as digital versions of conventional contracts, actual or implied or, worse, as mere automated settlement tools operating in a DLT environment.

It has been argued that the 'attack' on *The DAO* 'demonstrates the risk of disintermediation of financial services intermediaries that can result from DLT deployment', as well as 'the risk of flaws in smart contract coding, [and raises] questions about the application of the law to smart contracts'.[132] Perhaps more importantly, what the 'attack' on *The DAO* shows is that, conceptual considerations aside, and as a matter of public policy, there is no obvious interest in treating the Code as law, at least in the case of smart contracts: if the 'Code is law' doctrine were to be accepted here, acts similar to those perpetrated in the case of *The DAO* would not be treated as instances of abuse but, instead, as rightful actions, and as non-actionable incidents of the exploitation of particular features of a smart contract's computer code, to the actor's advantage. Such an outcome could be absurd, both because it would leave no room to interpret the genuine intentions of the parties to an electronic contract, and to deduce their presumed shared understanding of its conditions, and because it would exclude any scope for remedial action, aimed at reversing the real-world consequences of the operation of computer code. Conventional contracts that prove 'defective' can be amended, whether at the

[131] Allen & Overy LLP, 'Decentralized Autonomous Organizations', 2016 (Allen & Overy, 2016), 4-5.

[132] IOSCO, Research Report on Financial Technologies (Fintech), February 2017 (IOSCO, 2017), 58.

instance of the parties, or by operation of law: it is not readily obvious why smart contracts should be treated any differently.

4.3.3 Substantive law considerations

Whether or not a smart contract will qualify as an enforceable 'legal' contract will depend on the extent to which it incorporates each of the basic elements for the formation of a valid agreement, for the purposes of the national legal order in the context of which the question arises. There are at least three such elements of relevance to smart contracts, the non-fulfilment of any of which would presumably suffice to impede the recognition of their legal validity, namely, evidence of the contracting parties' *intention to create legal relations*, proof of the relevant *contractual terms*, and *external enforceability*. *The electronic-only manner of the creation of smart contracts* is another element worthy of attention here, both because certain types of contracts are subject to formality requirements and because digital contracts present specificities (*inter alia* in terms of their signature) that conventional contracts do not, and which may also be relevant to smart contracts.

It is against the above elements that this author would propose to measure, below, smart contracts, in terms of their alignment to their conventional peers.

4.3.3.1 Intention to create legal relations

The *intention to create legal relations* (and, through it, proof of the *consent* of the parties to be bound by the terms of an agreement) is universally accepted as one of the core elements for the formation of a valid contract.

Whether a DLT-enabled smart contract will satisfy this core element of a legally binding contract will depend not only on its terms but, also, on the *type of ledger* in which its software is embedded. While one may be prepared to accept that there can be something akin to a genuine 'meeting of minds' in the case of a smart contract written on a permissioned and/or proprietary ledger, accessible to the members of a restricted group who know (or can at least ascertain the identity of) and trust one another, it is more difficult to see how an intention to create legal relations can realistically be imputed to the members of an un-permissioned DLT platform, who ignore (and may be in no position to establish) the identity of the other participants, and who need not be deemed to be entirely indifferent to their risk profile, trading history or reputation, however much they may trust the contract formation process itself:[133] the freedom to choose one's counterparties is, after all, as much a

[133] Bonneau and Verbiest, 2017, at 77-78.

component of a valid contract as the freedom to decide whether to enter into a contract in the first place and, if so, subject to which terms and conditions.[134]

Another reason why it may be difficult to detect a genuine intention to create legal relations in the case of DLT-enabled smart contracts is linked to the absence, in their context, of the discretionary dimension of contract-making: it could be argued that the automated (or automatable) nature of smart contracts, and the exclusion of any human involvement in their formation (which, in the case of smart contracts, coincides with their actual execution) denies, *ipso facto*, the exercise of *any* measure of discretionary decision-making on the side of the parties to a smart contract (unless, that is, the counterparties have reserved for themselves the possibility to stop, by mutual consent, the execution of a smart contract); indeed, to the extent that the software in which smart contracts are embedded is *pre-programmed* to implement certain pre-agreed contractual terms, it could be argued that it operates under the contract law equivalent of 'duress', which, in the context of conventional contracts, is apt to serve as a vitiating factor, negating the existence of consent.

Although there is some force in it, this argument would appear not to countenance one key element: in the case of smart contracts, the contracting parties' intention to create legal relations is typically evinced simultaneously with its actual execution (proof, *par excellence*, even if only by *conduct*, of the parties' consent to contract with one another):[135] to separately look, in the context of smart contracts, for evidence of the parties' intention to create legal relations is to misunderstand the mechanics of the formation of smart contracts, which differ from those of conventional contracts on account of their automation and which, in essence, represent their main novelty and their core attraction. The automation of smart contracts is bound to have an impact on the process of their conclusion and performance, but it need not necessarily affect their legal nature *qua* contracts.

4.3.3.2 Certainty of contractual terms

Certainty as to the terms subject to which the contracting parties have agreed to create legal relations is an element that most legal systems will treat as crucial for the assessment of the legally binding effect of any bilateral arrangement intended to produce legal effects.

It has aptly been argued that, 'smart contracts that purely digitise a particular process but do not include, or operate in conjunction with, contractual terms (express or implied)' may not give rise to valid contracts, in the legal sense of the term, and that the same is true of 'follow-on contracts' that merely seek to implement *prior*

[134] It has nevertheless been argued that, for certain types of contracts, the intention to enter into contractual relations need not invariably be negated by the absence of a specific natural or legal entity to which a contracting party's offer would each time be extended: the example of automatic vending machines (the primordial illustration of a smart contract) is a case in point, and the same is true of all ordinary contracts of adhesion entered into between public transport companies or parking facility operators and their respective customers, to name but a few (see Lauslahti et al., 2017, at 10 and 14).

[135] Lauslahti et al., 2017, 16.

agreements, whether these are incorporated in a traditional or in a smart contract.[136] Besides, it is undisputed that the encoding of complex commercial contracts, which may include language that does not lend itself to a single, clear and unambiguous interpretation,[137] intentionally introduced by the contracting parties to capture nuances of significance to them or to afford them flexibility in their dealings, may prove difficult (especially if the parties have not reserved for themselves the option of encoded 'checkpoints', allowing for the exercise of discretion). Similarly, knowing *where* to look for the concrete terms of a smart contract may not always be as straightforward a task as in the case of a conventional contract, as the terms of a smart contract may be included both in the software in which the contract is written and in the rules of the platform that is hosting it, raising the prospect of conflicts between the two, of uncertainty in terms of how to address such conflicts, and of added costs to resolve them (e.g. by obtaining expert advice). The implication of the above is that, depending on their complexity,[138] certain contractual arrangements may not be convertible into smart contracts if relevant information is not to be lost in the process of their conversion from natural language into computer code and, more importantly, if they are not to lack the degree of clarity expected of any free-standing contractual agreement; and that certainty in terms of the contents of a smart contract need not always be attainable without access to sources external to the software of the smart contract itself.

If it is true that certain types of transactions cannot be reduced to smart contracts, whether on account of their complexity or because of their (regulated) subject matter,[139] and if certain smart contracts may not purport to incorporate the entire commercial arrangement governing dealings between two parties, this is not to say that, *as a class*, smart contracts cannot be the source of legally enforceable, contractual obligations: it is only on a case-by-case basis that it may be possible to determine whether a given smart contract comprehensively incorporates the terms and conditions subject to which the contracting parties have agreed to create legal relations. In particular, it is difficult to see why relatively simple contracts, such as those for the sale of goods, cannot be automated and processed through a distributed ledger, with the intention that they bind their parties (just as a conventional contract would), or why a smart contract cannot incorporate, by reference, external legal rules to complement its own, thereby achieving the requisite degree of certainty of terms.

---

136 Fulbright, 2016, 16.

137 Examples include references to 'compelling circumstances', 'undue delay', 'material deviation' and 'satisfactory performance', which lack a fixed meaning, and whose inclusion in contractual documentation often seeks to afford the contracting parties a certain margin of discretion in the appraisal of their contractual relations.

138 The legal magnitude of Blockchain: 'It is not the legal term itself that defines the level of complexity, but rather, it is the relation between the legal term and the ever-changing outside world that defines the level of scrutiny required in applying the law'.

139 The reference is, for instance, to contracts for the conveyance of land, which tend to be subject to formality requirements in many jurisdictions.

4.3.3.3 External enforceability

At its most basic, a 'contract is a promise or set of promises *that the law will enforce*' [our emphasis].[140] Herein lies one possible objection to treating smart contracts as *stricto sensu* 'legal' contracts. Unlike conventional contracts, which invariably operate by reference to a specific external legal framework, and which a court of law (or an arbitrator) will enforce, at the request of the parties, in the event of a dispute between them, smart contracts will automatically enforce *themselves* and, what is more, they will purport to do so *independently* of an external legal framework. It follows that, *a priori*, the very technology that underlies smart contracts would appear to pose enforceability issues (especially where such contracts would be embedded on un-permissioned Blockchains, lacking a central controlling authority and an arbitrator to resolve potential disputes). What is more, the concern with the enforceability of smart contracts is a valid one, notwithstanding their self-executory nature: an automated (or automatable) contract is apt to give rise to a dispute between its parties, in the same way that a conventional one can, in which case one would imagine the parties thereto to have an interest in accessing an arbitrator or a judicial instance to interpret and enforce its terms.

Despite the self-executory nature of smart contracts, the rules laid down in one or more external legal frameworks relevant to their performance are bound to apply to them, in the event of a dispute. While the author is not aware that, at the time of writing, courts had been confronted with questions of relevance to the enforcement of smart contracts, it is difficult to imagine that there would be anything to stop the judiciary from applying to smart contracts the prescriptions and dictates of domestic contract law, whether to reverse an unintended outcome or to remedy the consequences of a software error or to make a contracting party whole. From the perspective of their enforcement, smart contracts need not be as fundamentally different from conventional contracts as some of their advocates or detractors may assert: even if they are not backed, *a priori*, by a judicial enforcement mechanism, buttressed by legal doctrine and case law, this is not to say that they are impervious to the law or immune from the administration of the justice system. The author need not elaborate on the public policy implications of accepting a contrary conclusion. That their interpretation, as a condition precedent to their enforcement, may pose practical difficulties and require costly expert advice, is undisputed: but this is a distinct question to that of their enforceability, which is a matter of legal principle rather than practical expediency.

The illusion that smart contracts are solely administered by their computer code could, unless cleared, adversely affect the appetite of financial actors to resort to smart contracts to organize their economic interactions, especially for more complex or larger value transactions: it is unlikely that financial actors will be willing to risk

[140] A. Guest, (ed), *Chitty on Contracts* (27th edition, Sweet and Maxwell, 1994), 1.

losing the benefit of the protection afforded to them by contract law,[141] merely to reap the benefits of smart contracts, such as they are, unless the latter were to embody solid dispute resolution mechanisms of their own, which the parties could rely on if necessary.[142]

4.3.3.4 Impact of the electronic creation of smart contracts on their validity

The digital/electronic form of smart contracts could be perceived as a potential impediment to the recognition of their legal validity and enforceability, and this could well be in the case of contracts that, mostly for reasons of public policy, may have to comply with specific formalities as a condition precedent to their valid creation (such as contracts for the conveyance of land). What about other types of contracts?

Electronic contracts are not strangers to either the EU or the US legal orders, which already recognize as valid and enforceable contracts entered into digitally, without support from a conventional, written agreement between the contracting parties. Besides, despite the fact that, at the time of writing, no court had, to this author's knowledge, tackled the issue specifically with regard to smart contracts, there was a wealth of judicial precedent for the proposition that agreements intended to serve as a source of binding obligations are no less enforceable merely on account of the fact that they have been concluded through electronic means, as in the case of so-called 'clickwraps'.[143] For its part, in a bid to boost interest in E-Commerce, by ensuring that users can electronically sign contracts as a means of guaranteeing their enforceability, (UNCITRAL adopted, already in 1996, the Model Law on Electronic Commerce, Article 5 of which provides that '[I]nformation shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message'.[144] It follows that no obvious, conceptual obstacle to the validity of smart contracts is to be derived from the mere fact that these may only exist in digital format: in this particular sense, smart contracts are by no means a novelty, neither for the contemporary legal system nor for contracting parties.

A related issue, which could be perceived as an additional stumbling block to treating smart contracts on a par with conventional contracts, is the issue of *legal capacity* to enter into contractual relations. Given their electronic formation, certain smart

---

[141] It has aptly been observed that, 'the legal system ensures the existence of a public, transparent and explicit set of *universal* rules, whose legitimacy can easily be put into question. In contrast, regulation by code is elaborated mostly by private actors, who incorporate a set of *arbitrary* rules into technical artefacts, without any public purview and often without giving the opportunity for people to put these rules into question (this is especially true in the case of proprietary software that does not publish its source code)', Filippi and Hassan, 2016, 12). These protections explain the inclusion of governing law and jurisdiction clauses in conventional contracts, so as to enable the contracting parties to benefit from the substantive law and procedural protections afforded by national legal systems, including those to which the contracting parties may have no obvious link.

[142] Fulbright, 2016, 19.

[143] The reference is to agreements entered into online, often in connection with software licenses, under the terms of which end-users are required to signal their acceptance of certain contractual terms and conditions by clicking on an 'I Agree' button in a pop-up window or dialog box.

[144] Article 6 further states that, '[W]here the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference', while Article 7 provides for the recognition of electronic signatures.

contracts (and especially those entered into on un-permissioned platforms) could, as a practical matter, make it difficult to ascertain the identity of contracting parties, and to establish their legal capacity. The electronic creation of smart contracts could also raise a different form of legal capacity-related concern, linked to the difficulty of ascertaining the identity of one's contracting parties and, in particular, whether these are human agents or, instead, robots: at the time of writing, the latter were not recognised as separate legal personalities of their own, and could not, *de lege lata*, enter into valid and enforceable smart contracts, whether *inter se*, or with a human agent.[145]

While the above concerns are valid, they are of a practical rather than of a legal nature: the enforceability of a smart contract will turn on the extent to which it fulfils the exact same legal capacity-related conditions as any other, conventional contract, but not on its inherent features *qua* smart contract or the (electronic) manner of its formation, however much the latter may pose legal capacity-related challenges.

4.4 Smart contracts: other legal challenges and possible solutions

Even if, for the reasons explained above, smart contracts *are* capable of producing legal effects, analogous to those of conventional contracts, they are also bound to give rise to novel risks. These risks can be broken down, for analytical purposes, into *two* heads, namely *loss of control over contractual outcomes* and *operational risks* (including legal risks proper).

Loss of control over contractual outcomes is a direct consequence of the automatable, pre-programmable nature of smart contracts. As soon as the pre-determined trigger event has materialized, computer code will effect direct and immediate changes on the securities and/or cash accounts held in a ledger. On account of their pre-determined nature, smart contracts are not capable of adjusting contractual outcomes to shifts in the contractual context or in the objective circumstances surrounding the performance of contractual agreements or to un-anticipated events[146] nor, in fairness, have they been conceived with the intention that they should.

Smart contracts can also give rise to operational, including legal, risks. Starting with *stricto sensu* operational risks, it is submitted that there are two sub-heads thereof. One is the risk that the software in which a smart contract is embedded proves to be defective. It has rightly been stated in this regard that, '[S]mart contracts in theory reduce human error through automation. However, if an error occurs, it is more difficult to resolve as the operations are linked and embedded in the blockchain, and are self-executing according to the code written in the smart contracts. Also, smart

[145] It is conceivable that, the more automated a process becomes, the link to real human beings or real legal entities will weaken, meaning that, in case of disputes, it may become less straightforward to point to a person or entity that is to be sued.

[146] See IOSCO, 2017, 51-52.

contracts introduce a different type of human error: coding error. The programming code of the smart contract may not accurately reflect human contractual intent and may thus be a source of operational risk.'[147]The second sub-head of operational risk peculiar to smart contracts is associated with their reliance on external outputs (such as, for instance, the price of stock, relevant to the exercise of an option for its purchase written on a smart contract): to the extent that smart contracts rely on such external outputs, their execution is vulnerable to erroneous information, casting doubts on their autonomy, self-sufficiency and, ultimately, reliability as reflections of the agreement of the contracting parties.

Turning to legal risks proper, we have explained earlier in this paper some of the reasons why smart contracts are likely to raise legal concerns. Foremost among them is the question of whether a particular smart contract can be the source of rights and obligations for its parties. But even if that particular issue were to be resolved in respect of a specific smart contract, a host of *other* legal issues would remain, all of which would be relevant in considering the overall legal risks associated with the use of smart contracts in a financial services context. These would include, a) whether smart contracts should be accessible to all or only some counterparties e.g. for reasons of consumer protection; b) the impact of the use of smart contracts by public authorities, including central banks, on their ability to fulfil their public tasks;[148] c) certainty in terms of the finality of payments or securities transfers facilitated through the use of smart contracts;[149] d) challenges in terms of ensuring compliance with AML/CTF rules in the context of smart contracting on unrestricted networks, and of imposing administrative and/or criminal sanctions in respect of the execution of automated transactions with an adverse effect on the market e.g. because they constitute market abuse;[150] e) the modalities for the interpretation of smart contracts, the manner of the appraisal, by courts, of their evidentiary status, and the choice of the legal system (or systems) by reference to which these issues would be resolved, in a scenario where multiple parties, operating out of multiple jurisdictions, enter into transactions facilitated through smart contracts; f) the impact of the self-executing and self-enforceable nature of smart contracts on the application of classic contract law doctrines and remedies (such as voiding contracts on grounds of duress, mistake, misrepresentation, unconscionability or a change in circumstances rendering their performance impossible, amending contracts due to changes in circumstances, or relying on the doctrines of apparent and ostensible authority to assess legal capacity to enter into a contract);[151] g) the detection of software defects, and the attribution of liability for

147 Ibid., 62.

148 The use of automated technologies entails some loss of discretion. One would, therefore, need to consider whether such loss can lead to undesirable outcomes and, eventually, to a loss of the discretionary powers necessary for the fulfilment of certain public tasks.

149 Payments or transfers of securities that have been pre-programmed long before certain events, such as insolvency, occur, may lead to questions about the validity of such payments and transfers; specific rules protecting such transactions may be necessary to create legal certainty.

150 For instance, it is not clear how AML/KYC obligations can credibly be performed in the context of public blockchain transactions, where there is only limited ability to identify one's counterparties.

151 Mills et al., 2016, 28-29.

them;[152] and h) the impact on data confidentiality of the inclusion, on a public ledger, of transaction information, including money flows and pricing.

Legal concerns aside, smart contracts are also apt to give rise to regulatory challenges, both because, through their potential to facilitate the creation of automatable, peer-to-peer variations of service platforms, they would deny regulators a central focal point on which they can attach regulatory compliance duties, and because their use is bound to give rise to consumer protection concerns, and to the need for safeguards to mandatorily be included in smart contracts to protect the legitimate interests of their contracting parties.

In terms of potential solutions to the above legal concerns, it has been suggested that the contracting parties may wish to use a complementary 'wrapper', to set out those of the terms of their bilateral agreement that are 'not deterministic and not suitable for execution through the smart contract', such as the 'right to terminate a contract or take a particular action because of the occurrence of a "material adverse event"'; the wrapper would prevail over the smart contract's software, in cases of conflict.[153] Another, similar 'work-around' is encapsulated in the idea of 'dual integration', i.e. in the linking of 'smart contracts and full legal contracts by reference to the contract's storage address on the blockchain'.[154] In terms of the regulatory response to some of the issues raised by the emergence of smart contracts, it is likelier than not that legislative protection will need to be envisaged and introduced, to implement existing or to extend new elements of consumer protection law to the parties to smart contracts, or to ensure that regulated entities, such as credit institutions, that are parties to smart contracts can fulfil their regulatory compliance duties when opting to automate some of their contractual interactions.

[152] The question is whether liability would attach to the software designers or to the operators of the distributed ledger on which a smart contract has been executed.

[153] See Lim, et al., 2016 (where it is also suggested that the smart contract should include a 'fail-safe' to allow its code to be terminated in certain pre-agreed situations, or amended, in cases of contract variation, or where a party chooses to waive some of its contractual rights).

[154] N. Kilbride, Enforcing Legal Smart Contracts, Monax, 2016.

5 Final remarks

Human societies depend on exchanges of value, and evolving consumer demands are bound to create demand for novel means of exchange, payment rails and value exchange enablers. The emergence of VCs, the debate surrounding the possible use of DLTs and distributed ledgers in a financial sector context, and the reflections on the scope for the deployment of smart contracts, are reflections of the quest for novel means of exchange, alternative payment rails and innovative financial transaction facilitators, not administered by single entities, nor backed by central payment mechanisms, nor centrally regulated.

In our account, above, of the preconditions for alternative payment media to establish themselves in the retail space, certain criteria were identified: lower (or no) intermediation costs, user-friendliness, wide acceptability in a broad spectrum of payments (irrespective of the type or value of the underlying transaction), instant settlement of the underlying fiduciary obligation, and protection from fraud or misuse. How do VCs, in general, and *bitcoin*, in particular, measure up to these criteria? For the reasons explained in this paper, *bitcoin* falls short of several of these criteria for, a) it only offers probabilistic settlement; b) it is energy intensive, c) the speed of the *Bitcoin* network transactions confirmation is low; d) it gives rise to regulatory frictions and legal classification concerns; and e) it is volatile. Whatever the concrete variation of the technology they deploy, other VCs and VC-related payment protocols should be expected to feature some, at least, of *bitcoin's* core elements (with an emphasis on the execution of payments/value transfers without recourse to intermediaries, and with transfers based, at least to some extent, on distributed trust between payment network participants). What this means is that other VCs would also share[155] some, at least, of the features and shortcomings of *bitcoin*. No less importantly, it is difficult to see how unpegged, privately-issued VCs, backed by no underlying State authority, and not representing claims against (or liabilities of) a trusted third party can enjoy legal tender status *unless* issued at the behest (or with the involvement) of a central bank or another, comparable public authority, whether as 'money' or as currency surrogates/substitutes. Is this to say that *bitcoin* and, by extension, other VCs, have no future as retail payment instruments? Not necessarily. Where one could expect *bitcoin* and other VCs to stand a chance of success in the retail space, as substitutes for established currencies, is as settlement media in markets where the local *fiat* currency may be volatile or where payment rails may either be unavailable, unreliable or far too costly, especially for the unbanked, but, also, as facilitators for foreign remittances (provided there are local outlets in the recipient's jurisdiction, willing to exchange VCs against *fiat* currencies).

[155] For instance, even if inspired by its *bitcoin* equivalent, the technology used by other VCs used for retail payments may differ from the *Blockchain* model used in *bitcoin*. While the latter is an open (or 'un-permissioned') system, where the transaction validation process is open to all nodes, permissioned-based technology is likelier than not to be used in the context of mass retail payments, making of validation the preserve of authorised participants, known to all network users.

Even if some (or most) of the VCs currently in use were to fade into oblivion, for failing to overcome the significant hurdles standing in the way of their more widespread acceptance, the *technology* that underpins them (or some variation of it) could find valuable uses, enabling financial sector innovation, in general, and payent sector innovation, in particular. What will be worth exploring, going forward, is whether the benefits and risks of *bitcoin* or other VCs are only relevant where a VC is recorded in a Blockchain-type ledger or whether some of those risks and benefits should also be expected to manifest themselves in the context of payments settled in *fiat* currencies, where a 'bridge' has been established between a Blockchain ledger recording digital assets, and a conventional ledger recording the transfer of *fiat* currencies used as settlement media.

Turning to DLTs, their success or failure, in a financial sector context, will ultimately turn *first* on their particular configuration (permissioned or un-permissioned), and *second* on whether their presence can help substitute commercial trust in third party intermediaries with trust in digital, distributed technology and computer code. Trust is a condition *sine qua non* for, and one of the foundations of, economic activity. For the reasons explained in this paper, un-permissioned DLTs raise a number of fundamental legal concerns, which would need to be overcome DLTs they can be used as substitutes for contemporary payment transaction processing platforms. Without regulatory intervention and international coordination, to overcome some, at least, of those issues, it is difficult to see how the use of un-permissioned ledgers, as the genuine bearers of the revolutionary promises of DLTs, could gain traction in a financial sector context; and that the need to ensure compliance with legal and regulatory requirements is bound to be an argument against full disintermediation, so as to preserve some degree of independent, third-party monitoring of the compliance of DLT platforms with basic legal requirements.

Finally, a few words are apposite on DLT-embedded smart contracts, and their promises, whether in the field of payments or beyond. The *first* of those promises is to facilitate the formation of contractual transactions that are incorruptible and tamper-proof, shielding their parties from the consequences of undesirable, malevolent external interference; the *second* is to provide a reliable record of the entire transacting history between the contracting parties; the *third* is to automate buy, sell and supply transactions; and the *fourth* is to decrease the marginal cost of contracting by, *inter alia*, disposing with time-consuming and resource-intensive formalities for the formation of contracts, promoting a measure of contractual standardization, and removing the ambiguities often built into contractual agreements drafted in natural (as opposed to computer) language. Even if it were to be accepted that they do not lack, as a class, the hallmarks of valid contractual agreements, despite the different mechanics of their creation and performance, smart contracts 'unavoidably change our understanding of contracts',[156] and raise a number of legal issues, with an impact both on their uptake and, no less importantly, on the policy and legal responses to their emergence. The need for regulatory intervention appears clear, both to create the environment of legal certainty

[156] Koulu, 2016, 55.

necessary for the use of smart contracts as means through which to facilitate automated payments and other, value exchanges, and to generate confidence among their user community in their ability to give effect to their contractual intentions.

Selected bibliography

Books

Abel, Andrew B. and Ben S. Bernanke, *Macroeconomics* (5th edition, Pearson, 2005).

Bonneau, Thierry and Thibault Verbiest, *Fintech et Droit* (Paris, RB Edition, 2017).

Fox, David, *Property Rights in Money* (OUP, 2008).

Guest, Anthony. G. (ed), *Chitty on Contracts* (27th edition, Sweet and Maxwell, 1994).

Haentjens, Matthias and Pierre de Gioia-Carabellese, *European Banking and Financial Law* (Routledge, 2015).

Lessig, Lawrence, *Code and other laws of the cyberspace* (Basic Books, 1999).

Proctor, Charles, *Mann on the Legal Aspect of Money* (7th edition, OUP, 2012).

Smith, G.J.H., *Bird & Bird, Internet Law and Regulation* (4th edition, Thomson/Sweet & Maxwell, 2007).

Vigna, Paul and Michael Casey, The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order (St. Martin's Press, 2015).

Contributions in edited volumes

Middlebrook, Stephen T. and Sarah Jane Hughes, 'Substitutes for Legal Tender: lessons from the History of the Regulation of Virtual Currencies' in J. Rothchild, (ed.), *Research Handbook on Electronic Commerce Law* (Edward Elgar, 2016).

Mik, Eliza, 'Formation Online', in M. Furmstrom and G. J. Tolhurst (eds), *Contract Formation: law and practice* (OUP, 2010).

Miller, Saul, 'Payment in an On-line World' in L. Edwards and C. Waelde (eds), *Law & the Internet* (Hart Publishing, 2000).

Straus, Ryan, J. and Matthew J. Cleary, 'The United States' in Stuart Hoegner (ed.), *The law of Bitcoin* (iUniverse, Bloomington, 2015).

Vereecken, Marc, 'Directive 98/26/EC on the European Union Payment Systems and Securities Settlement Systems', in *Settlement Finality in the European Union: The EU Directive and Its Implementation in Selected Jurisdictions*, M. Vereecken and A. Nijenhuis (eds), (Kluwer Legal Publishers, 2003).

Articles in journals

Bali, Mehdi, 'Les crypto-monnaies, une application des block chain technologies à la monnaie', *Revue de Droit Bancaire et Financier*, No 2 mars-avril 2016, pp. 14-19

Bayern, Shawn, 'Dynamic Common Law and Technological Change: The Classification of Bitcoin', *Washington & Lee Law Review Online*, (2014) 2, pp. 22-34

Bollen, Rhys, 'The Legal Status of Online Currencies: Are Bitcoins the Future?' *Journal of Banking and Finance Law and Practice*, (2013) 24, pp. 272-293

De Vauplane, Hubert, 'Bitcoin, monnaie de singe ou monnaie légale?' *Revue Banque*, juillet-août, 2013 no page numbers?

Geva, Benjamin, 'Virtual Currencies and Block Chains: Developments and Issues', *National Banking Law Review*, (2016) 35(3), pp. 36-42

Geva, Benjamin, 'Disintermediating electronic payments: digital cash and virtual currencies', *Journal of International Banking Law and Regulation*, (2016) 31(12), pp. 661-674

Gless, Sabine, Peter Kugler and Dario Stagno, 'Was ist Geld? Und warum schützt man es? Zum strafrechtlichen Schutz von virtuellen Währungen am Beispiel von Bitcoins', *Recht*, (2015) 2, pp. 1-16

Grinberg, Reuben, 'Bitcoin: An Innovative Alternative Digital Currency', *Hastings Science & Technology Law Journal*, (2012) 4(1), pp. 159-208

Guinier, Daniel, 'Monnaies virtuelles: le cas bitcoin; paradoxes et processus d'une crypto-monnaie', *Expertises*, février 2015, No 399, pp. 56-63

Kalderon, Mark, Ferdisha Snagg and Claire Harrop, 'Distributed Ledgers: A future in Financial Services'? *Journal of International Banking Law and Regulation*, (2016) 31(5), pp. 243-248

Koulu, Riikka 'Blockchains and Online Dispute Resolution: Smart Contracts as an Alternative to Enforcement', *SCRIPTed*, (2016) 13(1), May 2016, pp. 40-69

Kvarnström, Jimmy and Andreas Gustafsson, 'Blockchain: From Why to What and Regulating How', *International In-House Counsel Journal*, (2016) 9(36), pp. 1-7

Quest, David QC, 'Taking Security over bitcoins and other virtual currency', *Butterworths Journal of International Banking and Financial Law*, (2015) 7, p. 401

Raskin, Max I., 'Realm of the Bitcoin: Bitcoin and Civil Procedure', *Fordham Journal of Corporate and Financial Law*, (2015) 20, pp. 969-1011

Reidenberg, Joel, R., 'Lex Informatica: The Formulation of Information Policy Rules Through Technology', *Texas Law Review Volume*, (1998) 76(3), pp. 553-593

Rosner, Marcel T. and Andrew Kang, 'Understanding and Regulating Twenty-First Century Payment Systems: The Ripple Case Study', *Michigan Law Review*, (2016) 114(4), pp. 649-681

Roussille, Myriam, 'Le bitcoin: objet juridique non identifié', *Banque & Droit*, No 159, janvier-février 2015, pp. 27-31

Perkins, Joanna and Jennifer Enwezor, 'The legal aspects of virtual currencies', *Butterworths Journal of International Banking and Financial Law*, (2016), pp. 569-572

Sams, Robert, 'Bitcoin Blockchain for Distributed Clearing: A Critical Assessment', *The Capco Institute Journal of Financial Transformation*, (2015) 4, pp. 39-46

Wiseman, Scott A., 'Property or Currency? The Tax Dilemma Behind Bitcoin', *Utah Law Review*, (2016) 2, pp. 417-440

Institutional publications

Ali, Robleh, John Barrdear, Roger Clews and James Southgate, 'Innovations in payment technologies and the emergence of digital currencies', *Bank of England Quarterly Bulletin 2014*, 3rd Quarter.

Dowd, Kevin, 'New Private Monies: A Bit-Part Player?' *Institute of Economic Affairs*, London, 2014, pp. 7-37.

He, Dong, Karl Habermeier, Ross Leckow, Vikram Haksar, Yasmin Almeida, Mikari Kashima, Nadim Kyriakos-Saad, Hiroko Oura, Tahsin Saadi Sedik, Natalia Stetsenko, and Concepcion Verdugo-Yepes, Virtual Currencies and Beyond: Initial Considerations, *IMF Staff Discussion Note*, SDN/16/03, January 2016.

Lauslahti, Kristian, Juri Mattila, Juri Seppälä, 'Smart Contracts – How will Blockchain Technology Affect Contractual Practices?' *ETLA Reports*, No 68, 9 January 2017.

Lo, Stephanie and Christina J. Wang, 'Bitcoin as Money? Current Policy Perspectives', *Federal Reserve Bank of Boston*, September 2014.

Lumpkin, Stephen A., 'Regulatory Issues Related to Financial innovation', *OECD Financial Market Trends*, Vol. 2009 (2).

Mcleay, Michael, Amar Radia and Ryland Thomas, 'Money in the Modern Economy: An introduction', *Bank of England Quarterly Bulletin 2014*, 1st Quarter.

McGrath, Noel, 'Transacting in a Vacuum of Property Law', Dickson Poon TLI, *King's College Research Paper Series*, Paper 22/2016.

Mills, David, Kathy Wang, Brendan Malone, Anjana Ravi, Jeff Marquardt, Clinton Chen, Anton Badev, Timothy Brezinski, Linda Fahy, Kimberley Liao, Vanessa Kargenian, Max Ellithorpe, Wendy Ng, and Maria Baird, 'Distributed ledger

technology in payments, clearing and settlement', *Finance and Economics Discussion Series 2016-095*, Board of Governors of the Federal Reserve System.

Pinna, Andrea and Wiebe Ruttenberg, 'Distributed ledger technologies in securities post-trading: Revolution or evolution?' *ECB Occasional Paper Series*, No 172/April 2016.

Yermack, David, 'Is Bitcoin a Real Currency?' *NBER Working Paper*, No 19747, December 2013.

Electronic sources

Athey, Susan, '5 Ways Digital Currency Will Change the World', *World Economic Forum Agenda*, 22 January 2015.

Barlow, John P., 1996, 'A declaration of the independence of cyberspace'.

Buterin, Vitalik 'A Next-Generation Smart Contract and Decentralized Application Platform, Ethereum', *White Paper*, 2013.

de Filippi, Primavera and Samer Hassan, 'Blockchain technology as a regulatory technology: From code is law to law is code', (2016) First Monday (21), p. 12.

Garay, Juan. A., Aggelos Kiayias and Nikos Leonardos, 'The Bitcoin Backbone Protocol: Analysis and Applications', 7 March 2017.

Kilbride, Nina, 'Enforcing Legal Smart Contracts', Monax.

Lim, Cheng, Callum Sergeant and T.J. Shaw, 'Smart Contracts: Bridging the Gap Between Expectation and Reality', *Oxford Business Law Blog*, 11 July 2016

Milne, Alistair 'Cryptocurrencies from an Austrian Perspective', April 17, 2017, pp. 7-8.

Nakamoto, Satoshi, 'Bitcoin: A peer-to-peer electronic cash system', November 2008.

Schwartz, David, Noah Youngs and Arthur Britto, 'The Ripple Protocol Consensus Algorithm', *Ripple Labs Inc.*, 2014.

Szabo, Nick, 'The idea of smart contracts', 1997.

Acknowledgements

The views expressed in this paper are attributable to its author and do not necessarily reflect those of the ECB or the Eurosystem. The author is most grateful to Klaus M. Löber, Andrea Pinna and Alistair Milne for their very helpful comments on earlier drafts of this paper. All remaining errors are those of the author. Unless otherwise stated, website references were accurate as of 11 October 2017.

Phoebus Athanassiou
European Central Bank, Frankfurt am Main, Germany; email: phoebus.athanassiou@ecb.europa.eu

Postal address	60640 Frankfurt am Main, Germany
Telephone	+49 69 1344 0
Website	www.ecb.europa.eu

ISSN	1830-2696 (pdf)	DOI	10.2866/201593 (pdf)
ISBN	978-92-899-3015-4 (pdf)	EU catalogue No	QB-YH-17-001-EN-N (pdf)