EBA/Op/2014/08

4 July 2014

# EBA Opinion on 'virtual currencies'

.

# Contents

**Executive summary** 5

**Background** 7

**Definition of virtual currencies and market participants** 10

Definition 11

Market participants 13

**Potential benefits** 16

Economic benefits 16

Individual benefits 19

**Risks, and their causal drivers** 21

Risks to users 23

Risks to non-user market participants 29

Risks to financial integrity 32

Risks to payment systems and payment service providers in FCs 35

Risks to regulatory authorities 36

**The proposed regulatory approach** 38

Summary of the key risk drivers 38

A potential regulatory approach for the long term 39

The immediate regulatory response for the short term 43

Legal basis for this Opinion 44

The rationale for a consistent regulatory response across the EU 45

# List of figures

Figure 1: Overview of risks 22

Figure 2: Overview of risk drivers 38

# Abbreviations

| | |
|---|---|
| **AMLD** | Anti-Money Laundering Directive |
| **CIS** | Collective Investment Scheme |
| **DGSD** | Deposit Guarantee Scheme Directive |
| **EBA** | European Banking Authority |
| **EMD** | Electronic Money Directive |
| **ETF** | Exchange Traded Fund |
| **e-wallet** | Electronic wallet |
| **FC** | (Conventional) Fiat currency |
| **IOU** | I owe you |
| **KYC** | Know your customer (requirements) |
| **MiFID** | Markets in Financial Instruments Directive |
| **PSD** | Payment Services Directive |
| **SEPA** | Single Euro Payments Area |
| **VC** | Virtual currency |

# Executive summary

One of the tasks of the EBA is to monitor new and existing financial activities and to adopt guidelines and recommendations with a view to promoting the safety and soundness of markets and convergence of regulatory practice. In September 2013, 'virtual currencies' emerged on the EBA's radar as one of the many innovations to monitor. Following three months of analysis, the EBA issued a public warning on 13 December 2013, making consumers aware that VC are not regulated and that the risks are unmitigated as a result.

The question that remained unaddressed at the time was whether VCs should or can be regulated. This EBA Opinion sets out the result of this assessment and is addressed to EU legislators as well as national supervisory authorities in the 28 Member States.

VCs are a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a FC, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically. The main actors are users, exchanges, trade platforms, inventors, and e-wallet providers.

While there are some potential benefits of VCs, for example, reduced transaction costs, faster transaction speed and financial inclusion, these benefits are less relevant in the European Union, due to the existing and pending EU regulations and directives that are explicitly aimed at faster transactions speeds and costs and at increasing financial inclusion.

The risks, by contrast, are manifold. More than 70 risks were identified across several categories, including risks to users; risks to non-user market participants; risks to financial integrity, such as money laundering and other financial crime; risks to existing payment systems in conventional FCs, and risks to regulatory authorities.

Numerous causal drivers for these risks were identified too, as these indicate the regulatory measures that would be required to mitigate the risks. The risks include the fact that a VC scheme can be created, and then its function subsequently changed, by anyone, and in the case of decentralised schemes, such as Bitcoins, by anyone with a sufficient share of computational power; that payer and payee can remain anonymous; that VC schemes do not respect jurisdictional boundaries and may therefore undermine financial sanctions and seizure of assets; and that market participants lack sound corporate governance arrangements.

A regulatory approach that addresses these drivers comprehensively would require a substantial body of regulation, some components of which are untested. It would need to comprise, amongst other elements, governance requirements for several market participants, the segregation of client accounts, capital requirements and, crucially, the creation of 'scheme governing authorities' that are accountable for the integrity of a VC scheme and its key components, including its protocol and transaction ledge.

However, whilst such a 'long-term' regime is not in place, some of the more pressing risks identified will need to be mitigated in other ways. As an immediate response, the EBA

recommends that national supervisory authorities discourage credit institutions, payment institutions and e-money institutions from buying, holding or selling VCs.

The EBA also recommends that EU legislators consider declaring market participants at the direct interface between conventional and virtual currencies, such as virtual currency exchanges, to become 'obliged entities' under the EU Anti Money Laundering Directive and thus subject to its anti-money laundering and counter terrorist financing requirements.

This immediate response will 'shield' regulated financial services from VC schemes, and will mitigate those risks that arise from the interaction between VC schemes and regulated financial services. It would not mitigate those risks that arise within, or between, VC schemes themselves.

Other things being equal, this immediate response will allow VC schemes to innovate and develop outside of the financial services sector, including the development of solutions that would satisfy regulatory demands of the kind specified above. The immediate response would also still allow financial institutions to maintain, for example, a current account relationship with businesses active in the field of VCs.

# Background

1. One of the tasks of the EBA, in accordance with Article 9 of its founding regulation, is to monitor new and existing financial activities and to adopt guidelines and recommendations with a view to promoting the safety and soundness of markets and convergence in regulatory practice.

2. In September 2013, virtual currencies (VCs) emerged as one of the many innovations the EBA was monitoring at the time. VCs are a digital representation of value that is neither issued by a central bank or public authority nor necessarily attached to a FC, but is accepted by natural or legal persons as a means of exchange and can be transferred, stored or traded electronically.

3. In their decentralised variant, VC schemes tend to be created online using powerful computer hardware, which allows users to 'mine' small amounts of the currency by solving deliberately complex algorithms. The increase in the supply of VC units in the decentralised VC schemes that exist is said to be fixed by a mathematical protocol. Only small amounts are released over time, and the computing power required to mine a unit increases over that time. Miners validate VC transactions and tend to operate anonymously, from anywhere in the world.

4. VC units can also be bought at exchanges using conventional FC, such as the euro, the pound sterling or the US dollar. VC units are held in personalised accounts known as an electronic wallet (e-wallet). Using this wallet, consumers can send VCs online to anyone else willing to accept them, or convert them back into FC. Each transaction is validated and recorded on a transaction ledger often referred to as a block chain.

5. At present, the size of all VC schemes is difficult to gauge, due to the uncertain reliability of the data sources. It is also unknown how many VC transactions are carried out, not as a means of payment but as a mere exchange between VC and FC. Using a generous interpretation, the number of global VC transactions has never exceeded 100 000 per day across the globe,[1] compared to approximately 295 million conventional payment and terminal transactions per day in Europe alone (i.e. credit transfers, direct debits, e-money transfers, cheques, etc.).[2]

6. In autumn 2013, however, the EBA noticed increased VC activity across EU Member States, with a growing number of VC schemes being launched, an increasing number of merchants, and a rising number of individuals using VCs, and Bitcoins in particular, not only as an

[1] See for example, http://blockchain.info/charts/n-transactions?timespan=1year&showDataPoints=false&daysAverageString=7&show_header=true&scale=0&address

[2] Which are equivalent to EUR 94.5bn per year, see http://sdw.ecb.europa.eu/reports.do?node=1000001439

investment but as a means of paying for goods and services. Market participants were apparently drawn to VCs because of the benefits of being able to transfer VC units peer-to-peer without the need for an intermediary. Given that the regulation of payment services and relevant EU directives – such as the Payment Services Directive (PSD) and the Electronic Money Directive (EMD) – fall into the EBA's scope of action, the EBA began assessing the phenomenon.

7. Following three months of analysis of the potential risks to individuals arising from using VCs, the EBA issued a public warning on 13 December 2013, making consumers aware that they may lose their money on an exchange, that their VC units may be stolen from their digital wallets, that they are not protected when using VCs as a means of payment, that the value of VCs has been very volatile, that transactions in VCs may be misused for criminal activities and that individuals holding VCs may be subject to unforeseen tax liabilities.[3]

8. In the months following the publication, several of the risks that had been highlighted in the warning started to materialise, as a market-leading exchange (Mt. Gox) had to close due to mismanagement, cyber-attacks and theft of a substantial amount of Bitcoins. As the most popular VC scheme at the time, the value of Bitcoins fluctuated wildly, and several jurisdictions changed the tax status of VCs.

9. However, VC schemes tend to have properties that are very similar to those provided by conventional payment service providers, as regulated and supervised by the EBA and the national supervisory authorities across the 28 EU Member States. The question yet to be addressed was whether VCs therefore should, or could be regulated.

10. The question was given further impetus because a few national jurisdictions, within the EU as well as beyond, began to take national approaches that deviated from one another. Some jurisdictions considered imposing requirements on specific VC market participants as specified in existing legislation or regulations, while others created new licensing requirements. Others still decided to ban financial institutions from interacting with VCs.

11. To find a solution to the issue of whether VCs can and ought to be regulated, the EBA carried out additional analysis during the first half of 2014, the results of which are presented in this EBA Opinion. The first chapter specifies a definition of VCs and identifies the main actors participating in the markets for VCs, such as users, exchanges, trade platforms, inventors, e-wallet providers and others. This is followed by a chapter specifying the potential benefits, such as transaction costs, transaction speed and financial inclusion outside of the EU.

12. The report continues by identifying the main risks arising from VCs, separated into risks arising to individuals, to other market participants, to financial integrity, to existing payment systems in conventional FCs, and to regulatory authorities. Each of the 70+ risks identified is tentatively prioritised based on indicative judgements of the probability of their

[3] See http://www.eba.europa.eu/-/eba-warns-consumers-on-virtual-currencies

materialisation and the impact of this materialisation. The causal divers are also identified for each risk, as these will indicate the regulatory measures that would be required to mitigate the risk drivers.

13. The final chapter concludes by proposing an immediate regulatory response as well as a potential response for the long term.

# Definition of virtual currencies and market participants

14. At the time of writing this report, more than 200 different VC schemes are said to be in circulation,[4] and many more are expected to be developed in the future, some of them with features that are not predictable at present. While this creates challenges when specifying definitions that are useful for the development of a regulatory approach, some differentiating features that should withstand the test of time can be identified nevertheless. These are specified in this chapter.

15. The same challenge arises when identifying the actors that participate in the market for VCs who would be the parties affected by any regulations developed. Many different types of actors are vying to be the first to offer innovative ancillary VC services of one kind or another, such as automated machines used to exchange VC against FC and vice versa, the possibility to revere charges, etc. It is uncertain which service offerings will emerge in the future, which ones will gain market acceptance and which underlying business models will therefore survive. Again, however, some key market participants with functions that create particular risks can be identified for regulatory purposes. These are also specified in this chapter.

16. Finally, it must be noted that VCs existed long before the more recent emergence of the decentralised VCs that this report focuses on. Early examples of centralised VCs that were not convertible to FCs (such as World of Warcraft Gold or frequent flyer miles), unidirectional convertible VCs (such as the former Facebook Credits or Linden Dollars) and bidirectional convertible centralised VCs (E-gold or Liberty Reserve). Originally, the desire for these currencies arose because members of a virtual community, such as a video game, were looking for a convenient way to reward the users, as well as to enable other financial transactions with the users.

17. Today, the size of all VC schemes, in aggregate as well as relative to conventional payment services, is difficult to gauge due to the uncertain reliability of the data sources. It is also unknown how many VC transactions are carried out, not as a normal payment but for a currency exchange between VC and FC. However, even if interpreted very generously, the number of Bitcoin transactions, which accounts for the vast majority of VC transactions, has never exceeded 100 000 per day across the globe,[5] compared to approximately 295 million conventional payment and terminal transactions (i.e. credit transfers, direct debits, e-money transfers, cheques, etc.) per day in Europe alone.[6]

[4] See, for example, http://coinmarketcap.com/

[5] See for example, http://blockchain.info/charts/n-transactions?timespan=1year&showDataPoints=false&daysAverageString=7&show_header=true&scale=0&address

[6] Which are equivalent to EUR 94.5 billion per year, see http://sdw.ecb.europa.eu/reports.do?node=1000001439

## Definition

18. This document concerns the phenomenon commonly referred to as 'virtual currencies'. As will become evident, the usage of the term 'currency' is misleading for several reasons, including the insinuation that it is therefore exchangeable against other currencies, which may not necessarily be the case. However, this document will not suggest a different denomination but, to reflect the common public usage of the term, will retain this term throughout the document.

19. VCs are defined as a digital representation of value that is neither issued by a central bank or public authority nor necessarily attached to a FC, but is used by natural or legal persons as a means of exchange and can be transferred, stored or traded electronically.[7] VCs can therefore be characterised along the distinguishing features specified below. Although some of the features resemble activities or products that are already within the remit of the EU E-Money Directive, these products are not intended to be included here, as e-money is a digital representation of FC, which VCs are not.

### A digital representation of value

20. This part of the definition refers to the fact that the value is essentially represented in digital form. This does not exclude the possibility that it may also be physically represented, such as through paper printouts or an engraved metal object. The term 'digital representation of value' is close to the monetary concept of a 'unit of account' but includes the option to consider VCs as private money or a commodity. It also avoids making reference to a standard numerical unit of account for the measurement of value and costs of goods, services, assets and liabilities, which might (according to some views), imply that it needs to be stable over time.

### Not issued by a central bank or a public authority, nor necessarily pegged to a fiat currency

21. This element of the definition differentiates VCs from FC issued by central banks or public authorities. Currency issued by a central bank or public authority is considered FC, regardless of its (physical or digital) form. The difference between electronic money and a virtual currency is that the latter is not necessarily attached to a FC, i.e. it does not have a fixed value in a FC and, furthermore, is not necessarily fixed to be redeemed at par value by an issuer. Electronic money, by contrast, means electronically, including magnetically, stored monetary value as represented by a claim on the issuer, which is issued on receipt of funds

[7] It 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.

for making payment transactions, and which is accepted by a natural or legal person other than the electronic money issuer.[8]

### Used by natural or legal persons as a means of payment

22. VCs can be used as a 'medium of exchange' to obtain goods and services from one holder, such as a private person or company, to another. This avoids the inconveniences of a barter system, i.e. the need for a coincidence of wants between the two parties involved in the transaction. How widely a VC scheme is accepted amongst market participants (i.e. its acceptance network) varies from scheme to scheme and could deliberately be designed to be for broader or for more limited use (e.g. for a specific community of individuals).

### Can be transferred, stored and traded electronically

23. VCs can be (i) transferred from one user to another via electronic means, (ii) stored on an electronic device or server and (iii) traded electronically. However, it does not exclude physical transfers, the storage of copies in other forms (e.g. paper, minting and engraving) or that the VC is traded in other ways. Furthermore, the potential function of VCs as a 'store of value', i.e. that the value can be saved and retrieved in the future, does not necessarily imply that the value will remain stable over time and will not be subject to inflation or deflation.

24. The aim of the above definition is to distinguish VCs from (fiat) currency and, in particular, from e-money as digital representation of FC. In economic theory, money performs three different functions: (1) a unit of account, (2) a means of exchange and (3) a store of value. In principle, VCs could potentially fulfil one or more of the functions of money. However, the definition of VC above reflects the fact that these functions are, at least currently, not comparable in terms of quality, and are not always fulfilled at the same time as each other or to the same extent. Furthermore, from a regulatory perspective, inclusion of the term 'currency' in the denomination 'VC' is misleading as it implies the highest liquidity of the asset, wide or universal acceptance within its geography, as well as exchangeability with other (virtual and fiat) currencies, which may not necessarily be the case for every single VC scheme.

25. A number of additional characteristics can be identified for some of the VCs that currently exist, as outlined below. These are, however, not distinguishing features since either they do not apply to all VCs or it cannot be stated conclusively that they are applicable to all possible variant of VCs in the future.

### No legal tender status

[8] See Article 2.2 of the Electronic Money Directive (EMD), at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32009L0110

26. VCs are not legal tender, which means the following features are not fulfilled: (a) mandatory acceptance, i.e. that the creditor of a payment obligation cannot refuse currency unless the parties have agreed on other means of payment; (b) acceptance at full face value, i.e. the monetary value is equal to the amount indicated; and (c) that the currency has the power to discharge debtors from their payment obligations.

27. Currently, no VC has legal tender status in any jurisdiction, but it is theoretically possible that a VC might be declared legal tender in some jurisdictions in the future. However, this is unlikely to happen in an EU/EEA member state, and if it was issued by a public authority, it would cease to be a decentralised VC and would instead become a FC backed by a central authority.[9]

### Central versus decentralised scheme

28. Some VCs are issued and controlled by an individual or a group of individuals, while other VC schemes are issued and operated in a decentralised manner.

### Convertibility

29. Some VCs are convertible (or open) and, therefore, can be exchanged back-and-forth for fiat money at an exchange rate, whereas others are non-convertible (or closed), i.e. are specific to a particular community and cannot be exchanged for fiat money under the rules governing its use.

### Non-redeemable

30. This refers to the observation that, unlike electronic money, a VC, particularly in its decentralised variant, does not represent a claim on the issuer.

## Market participants

31. While at present a broad list of potential VC actors can be identified, not all of them necessarily need to be regulated. The more probable addressees for regulation are specified below.

### Users

32. A user is a person or legal entity that obtains VC and uses it to purchase real or virtual goods or services, or to send remittances in a personal capacity to another person (for personal use), or who hold the VC for other purposes, such as an investment. Typically users can obtain VC in one of the following three ways:

[9] The legal tender status of euro banknotes and coins is laid down by Article 128 (ex-Article 106 of the EC Treaty) of the Treaty on the Functioning of the European Union (TFEU). Exclusive right to authorise the issue of banknotes and approve coin volume issuance within the European Union is given to the European Central Bank. It would be necessary to amend the TFEU if a VC were declared legal tender.

- obtaining VC, for example through an exchange (or, for most centralised VCs, directly from the entity governing the scheme) using FC or some other VC;
- engaging in specific activities, such as responding to a promotion, completing an online survey, 'mining' (running special software to solve complex algorithms to validate transactions in the VC system); and/or
- receiving VC from the scheme governing entity, the issuer or another user who is acting for purposes other than his or her trade, business or profession.

### Merchants

33. A merchant is a user in a trade, business or professional role who accepts VCs in exchange for goods and services.

### Scheme governance authorities

34. A scheme governance authority is a legal person establishing and governing the rules for the use of a VC scheme, maintaining a central payment ledger, and who is responsible for the integrity of the scheme. In a centralised VC scheme, the scheme governance authority is also the issuer and therefore also has the authority to withdraw the VC from circulation.[10]

### Exchange

35. An exchange is a person or entity engaged in the exchange of VC for FC, funds or other brands of VC. Exchanges may generally accept a wide range of payments, including cash, credit transfers, credit cards and other VCs. Comparable to traditional currency exchanges, the larger VC exchanges provide an overall picture of the changes in a VC's exchange price and its volatility.

36. Some exchanges may offer services to their clients, such as conversion services for merchants who accept VCs as payment, but fear a depreciation risk and would immediately like to convert any incoming VC-payments into a (national) fiat money of their choice.

### Trade platforms

37. Trade platforms function as market places: they bring buyers and sellers of VCs together by offering them a platform on which they can offer and bid for VCs. Some trade platforms may even help their clients to locate merchants in their vicinity.

### Processing service providers

[10] The concept of governance authority is derived from the European Central Bank, *Harmonised oversight approach and oversight standards for payment instruments,* February 2009. Here the governance authority is described as being accountable for the overall functioning of the scheme that promotes the (initiation of the) payment instrument in question, and for ensuring that all the actors involved comply with the scheme's rules. Moreover, it is responsible for ensuring the scheme's compliance with oversight standards.

38. A processing service provider is an entity that facilitates the transfer of VC units from one user to another, usually through the means of information technology. In decentralised VC schemes, the provision of these services is sometimes rewarded by granting VC units to the provider, an activity that is referred to as 'mining' l.

### Wallet providers/custodians

39. Users may hold their VC accounts on their own devices or entrust a wallet provider to hold and administrate the VC account (an e-wallet) and to provide an overview of the user's transactions (via a web or phone-based service). With some VCs, the services entrusted to the wallet service provider may include the custody of the user's public and private key. Wallets can be stored both online ('hot storage') and offline ('cold storage'), the latter of which increases the safety of the balance by protecting the wallet.

### Inventors

40. An inventor is a person, or a group of people, who created or originated the concept of a particular VC and its underlying code and protocol.

### Technical service providers

41. A technical service provider is a third party providing additional (non-core) technical services that interact with the VC scheme through, for example, software applications, or to enable mining pool access.

### Information providers

42. An information provider makes available information on VC-related exchange rates, news feeds and other data.

### Miners

43. In decentralised VC schemes, miners solve deliberately complex algorithms to obtain small amounts of VC units. Miners tend to operate anonymously, from anywhere in the world, and validate VC transactions. When a group of miners controls more than half the total computational power used to create VC units, the group is potentially in a position to interfere with transactions, for example by rejecting transactions validated by other miners.

# Potential benefits

44. Supporters of VCs attribute numerous advantages to VC schemes. Some of these are more conceptual (such as financial inclusion), while others are more practical (e.g. transaction speed) or financial (e.g. lower transaction costs) in nature. What unites most of the advantages is that, at this stage of the development of VCs, many remain hypothetical, as the advantages have often not (yet) materialised.[11]

45. Listed below are the advantages that can conceivably be characterised as potential 'benefits', i.e. that could be objectively identified against a benchmark as an advancement for at least some market participants or for society more widely. Some of these benefits incur associated risks, which are also highlighted.

## Economic benefits

### Transaction costs

46. Due to the absence of intermediaries, VC transactions can currently be achieved at lower costs than other means of payment, such as payment cards or bank transfers. This is partly due to the absence of any regulatory requirements that would guarantee the safety of those means. VCs can also be less expensive for merchants as payees as well as for payers to whom transaction costs may be partially passed on. Although reliable and independent data on the exact costs of VC transactions is difficult to ascertain, some anecdotal suggestions have been made that average transaction fees on the Bitcoin network tend to be less than 0.0005 BTC, or 1% of the transaction amount.[12]

47. This compares with 2%-4% for traditional online payment systems or an estimated 8%-9% for remittance without involving bank accounts via money transmitters.[13] Transactions within or between VC schemes are also not subject to the exchange fees applied to conversions for transactions with third countries, therefore providing further potential for cost savings, (although conversion fees would typically apply as and when VC are exchanged against FC or vice versa). The increase in competition for transaction services may also have a cost-reducing effect on the costs of conventional transactions in FC.

[11] An exception may be regarding those market participants who have already taken advantage of the significant exchange rate volatility of VCs, or the anonymity feature that allows them to escape surveillance, purchase illegal goods, evade taxes, commit other forms of crime or avoid seizure of their assets. However, these are not considered to be benefits.

[12] Brito, J., *Beyond silk road: potential risks, threats, and promises of virtual currencies*, Testimony before the Senate Committee on homeland security and governmental affair, 18 November 2013, p. 11.

[13] Wu, R., *Why we accept Bitcoin*, Forbes, 13 February 2014, at http://www.forbes.com/sites/groupthink/2014/02/13/why-we-accept-bitcoin/, and World Bank, *Remittance Prices Worldwide,* 2014.

48. Unsurprisingly, the low transaction costs, as well as the high divisibility of VC units, make VC schemes a particularly attractive way to effect micropayments.

49. However, several caveats need to be made about these alleged benefits. Firstly, the cost advantages are not guaranteed, as miners of popular decentralised VCs such as Bitcoins currently tend to be compensated by both transaction fees and a share in recently mined VC units. It is reasonable to assume that, as the number of newly issued VC units decreases over time, miners will have to rely more on transaction fees to recoup their investment of processing power. It is therefore reasonable to assume that transaction fees will increase in the future.

50. Secondly, most merchants that accept VCs tend to convert them immediately into their local FC,[14] an activity that also incurs costs (estimated to be 1% of the amount to be exchanged).[15] Thirdly, the higher fees for other means of payment transactions are partly due to the regulatory requirements imposed on the regulated entities that provide them, as a result of security measures, corporate governance, internal control measures, prudential requirements and more. Should VCs schemes be regulated as a financial service, associated (although perhaps not identical) costs will inevitably impact upon VC service providers as well. These compliance costs will negate at least some of the cost advantages that VC systems are currently enjoying.

51. Finally, and most importantly, the cost differentials between FC and VC transactions referred to above are much less pronounced in the Member States of the European Union that are part of the Single Euro Payments Area (SEPA). The SEPA is the EU's payment-integration initiative for the simplification of bank transfers in euros. As of spring 2014, the SEPA consists of 34 countries, including the 28 EU member states. Furthermore, the EU regulation on the equality of charges for cross border payments eliminates the differences in charges for cross-border and national payments in euros.[16] As a result, the costs arising for payers and payees when making cross-border transactions through conventional payment services is already low or, indeed, free, therefore significantly reducing the cost advantages of VCs in Europe.

### Transaction processing time

52. Transactions using VCs can potentially be settled faster than those of FCs.[17] For Bitcoins, the total process time is said to be between 10 and 60 minutes. It is claimed that, on average, a new block is added every 10 minutes to the blockchain transaction ledger. In this respect, VC payments appear to compare favourably with credit transfers or card payments, particularly for payments between different currency areas. Also, processing VC payments takes place on a 24/7 basis, unlike payments made through traditional payment systems. However, for

[14] Krohn-Grimberghe, A. en C. Sorge, *Practical aspects of the bitcoin system*, Paderborn, Universität Paderborn, 2013.

[15] UBS, *Bitcoin and Banks. Problematic currency, interesting payment system,* 24 March 2014.

[16] See Regulation(EC) No 924/2009 at http://ec.europa.eu/internal_market/payments/crossborder/

[17] 'Virtual Currencies: The Legal and Regulatory Challenges', Global Forum on Law, Justice and Development and held at the World Bank's headquarters in Washington, DC on 14 June 2013.

similar reasons as explained above, these benefits are reduced for the 34 countries of the SEPA agreement, because the payee needs to be credited, at latest, by the next business day. Moreover, a number of countries around the world have already established several settlement cycles per day or even 24/7 real-time payment services. Furthermore, regarding card payment transactions, real-time authorisation transaction systems guarantee the payment to the payee.

### Certainty of payments received

53. VC schemes allow merchants to avoid having to refund transactions, particularly those that are based on an alleged non-fulfilment of a contract. In conventional FC payment systems in some jurisdictions, merchants have been reported to complain about large numbers of consumer-initiated payment charge backs that were based on false claims that a product had not been delivered.[18]

54. The downside of this benefit is that, for payers, the irrevocability of transactions does not allow consumers to be protected against error or fraud resulting from the merchant or other actors. These and other risks arising from the non-reversibility feature of VCs are specified in the subsequent chapter.

### Contributing to economic growth

55. Compared to traditional payment systems with established business actors, VCs have spawned new types of businesses that did not exist before. The use of decentralised VCs offers various new business opportunities. For example, the activity of mining has spawned the development of specialised mining hardware, specialised server farms, commercial mining services such as mining pools, as well as demand for safe storage capacities. Further business opportunities have arisen for exchanges and trade platforms, due to the need to convert VCs into FCs and vice versa. The main focus of innovation opportunities is the IT sector although they may also arise in the financial services sector.[19]

### Financial inclusion outside the EU

56. In jurisdictions where financial services are not widely available, where users have a high risk profile, where the national currency is not convertible into other FC, where financial services are too expensive for individuals, or where the administrative burden for obtaining an account is high, VC schemes provide an alternative way for individuals to achieve the same end: accessing commerce and effecting payment transactions.

57. However, this potential benefit is likely to be much less pronounced in the European Union, as directives such as the Payment Accounts Directive, adopted in April 2014 will provide

[18] Brito, J., *Beyond silk road: potential risks, threats, and promises of virtual currencies*, Testimony before the Senate Committee on homeland security and governmental affairs, 18 November 2013, p. 10.

[19] UBS, *Bitcoin and Banks. Problematic currency, interesting payment system,* 24 March 2014

cheap basic bank accounts for all citizens in the EU.[20] In contrast to VC, these accounts offer consumer protection and are subject to safeguarding requirements. The potential benefit is therefore more likely to advantage non-EU countries, especially in the case of money remittances, as VCs offer a less expensive alternative to conventional remittances that cost, on average, 8.36% of the amount sent.[21] Less developed countries may also benefit, for example by linking VC services to mobile payment services, allowing users to exchange their currency into Bitcoins via mobile phone.

58. However, this alleged benefit comes at a price, because VC schemes allow individuals, entities and jurisdictions that are subject to embargos or financial sanctions to circumvent those restrictions and participate in international trade and finance. Sanctions tend to be imposed on jurisdictions, and are therefore excluded from international finance because of a deliberate policy decision by a sovereign state or an intergovernmental organisation such as the EU or the UN, with a view to promote humanitarian or other political objectives. Consequently, the potential benefit also constitutes a significant risk of undermining an important policy tool of sovereign states, which is further explained in the chapter on risks below.

## Individual benefits

### Security of personal data

59. VC payment transactions do not require the provision of personal or sensitive data, unlike credit card data or passwords in the case of conventional payment methods. In this sense, VC units can be considered to be like cash: whoever possesses them also owns them, removing a source of potential identity theft.[22]

### Limited interference by public authorities

60. Some supporters of VCs consider FCs to be an untrustworthy means of payment due to governments' or central banks' power to control, and allegedly abuse, the supply of money denominated in that currency. [23]

61. However, while from a philosophical viewpoint, some people may argue that a system based on a central bank with the authority to influence money supply is not ideal, it does not automatically mean that a superior alternative is to have money supply set by an algorithm, as in decentralised VC schemes. On the contrary, as examined in great detail in the risks section below, the substantial exchange rate volatility illustrates that the depreciation of VC

[20] See http://ec.europa.eu/internal_market/finservices-retail/inclusion/index_en.htm

[21] World Bank, *Remittance Prices Worldwide*, March issue, 2014

[22] Wu, R., *Why we accept Bitcoin*, Forbes, 13 February 2014 http://www.forbes.com/sites/groupthink/2014/02/13/why-we-accept-bitcoin/.

[23] ECB, *Virtual Currency Schemes*, 2012, p. 22, box 2, at http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

units can be significantly greater in magnitude, and can also be much less predictable. The algorithm, protocol and transaction ledger might also be manipulated or might not be designed in good faith.

62. In summary, many of the potential benefits are likely to materialise outside the EU, in regions where the payment infrastructure may be less developed or less trustworthy.

# Risks, and their causal drivers

64. The main objective of a financial regulator is to identify risks arising from financial activities, prioritise them, and take mitigating action, if required. This chapter lists the risks that can arise from VCs and clearly identifies the bearer of the particular risk, the impact on the risk bearer in the event that the risk materialises, and the conditions needed for the risk to materialise. The causal drivers of the risks are also identified, as these will indicate the regulatory or supervisory measures that would need to be taken to mitigate the risks.

65. Finally, the risks are ranked into low, medium and high, in the interests of pursuing efficient and effective regulatory or supervisory intervention. However, the ranking is tentative because the phenomenon of VCs being assessed has not existed for a sufficient amount of time for there to be quantitative evidence available of the existing risks, nor is this of the quality required for a robust ranking.

66. Instead, the ranking is based on a tentative and preliminary assessment of factors such as the probability of a risk to materialise, the severity of the impact should the risk materialise, and an assessment of the anecdotal evidence available, such as bankruptcies of specific exchanges, cases of VC theft, etc.

67. Approximately 70 risks can be identified as arising from VCs. Some of these are similar, if not identical, to risks arising from conventional financial services or products, such as payment services or investment products, while others are specific to VCs. In the following, the risks are separated into risks to users, (indicated by the prefix A); risks to other market participants, (B); risks to financial integrity, (C); risks to payment systems in FCs, (D); and risks to regulators, (E). Where useful, a risk category may be further divided into sub categories. The risks are also numbered to facilitate additional analysis in subsequent chapters. An overview of all the risks is provided in Figure 1.

## Figure 1: Overview of risks

| | | ID | Risk description | Rank |
|---|---|---|---|---|
| A) Risks to users | General risks, irrespective of purpose | A01 | User suffers loss when an exchange is fraudulent | High |
| | | A02 | User suffers loss when an ostensible exchange is not a genuine exchange | High |
| | | A03 | User experiences drop in value of VCs due to (significant and unexpected) exchange rate fluctuation | High |
| | | A04 | User holding VCs may unexpectedly become liable to tax requirements | Med |
| | | A05 | User who is a member of a VC mining pool does not get fair share of mined VC units from a mining consortium | Low |
| | | A06 | User suffers loss when buying VCs that do not have the VC features that the user expects | Med |
| | | A07 | User's computing capacity is abused for the mining benefit of others | Low |
| | | A08 | User suffers loss due to changes made to the VC protocol and other core components | High |
| | | A09 | User is not in a position to identify and assess the risks arising from VCs | Low |
| | | A10 | User is in violation of applicable laws and regulations | Med |
| | | A11 | User loses VC units through e-wallet theft or hacking | High |
| | | A12 | User loses VC units when exchange gets hacked | High |
| | | A13 | User's identity may be stolen when providing identification credentials to access VCs | High |
| | | A14 | Market participants suffer losses due to unexpected application of law that renders contracts illegal/unenforceable | Med |
| | | A15 | Market participants suffer losses due to delays in the recovery of VC units or the freezing of positions | High |
| | | A16 | Market participants suffer losses due to counterparties/intermediaries failing to meet contractual settlement obligations | High |
| | | A17 | Market participants suffer losses of VC units held in custody by others | Med |
| | | A18 | Market participants suffer losses through information inequality regarding other actors | Med |
| | When used as a means of payment | A21 | User suffers loss when counterparty fails to meet contractual payment or settlement obligations | High |
| | | A22 | User experiences fraud or loss of FC when using VC cash machines | Med |
| | | A23 | User has no guarantee that VCs are accepted by merchants as a means of payment on a permanent basis | High |
| | | A24 | User suffers loss when VC payment they have made to purchase a good is incorrectly debited from their e-wallet | High |
| | | A25 | User is not able to convert VCs into fiat currency, or not at a reasonable price | High |
| | | A26 | User is unable to access VCs after losing passwords/keys to their e-wallet | High |
| | | A27 | User is not able to access VCs on an exchange that is a 'going concern' (i.e. has the resources to operate) | High |
| | | A28 | User is not able to access VCs on an exchange that has gone out of business (i.e. does no longer have resources to operate) | High |
| | When used as an investment | A41 | User suffers loss as a result of VC prices being manipulated | High |
| | | A42 | User investing in regulated financial instruments (e.g. derivatives, SPS, CIS) using unregulated VCs suffers unexpected loss | Med |
| | | A43 | User is misled by unreliable exchange rate data | Med |
| | | A44 | User suffers loss when investing in fraudulent VC investment schemes | Med |
| | | A45 | User is exposed to significant price volatility within very short time frames | Med |
| | | A46 | User cannot execute the VC exchange at the expected price | Med |
| | | A47 | User is exploited by a VC Ponzi scheme | Med |
| B) Risks to non-user market participants | Specific to exchanges | B11 | Exchange is operationally unable to fulfil payment obligations denominated in VCs or FCs | Med |
| | | B12 | Exchange is not in control of its operation | Med |
| | | B13 | E-wallet provider faces loss should their refund policies be abused to hedge currency transactions | Med |
| | Specific to merchants | B21 | After accepting VC for payment, merchant is not reimbursed | Med |
| | | B22 | Unlike a FC, the merchant cannot be certain that they can spend the VCs received | Med |
| | | B23 | The merchant cannot be certain of the FC purchasing power of the VCs they have received | Med |
| | | B24 | Merchant faces compensation claims from customers if transactions have been wrongly debited | Med |
| | Specific to some other market participants | B31 | Wallet provider loses e-wallets provided for individuals | High |
| | | B32 | Scheme governance authority fails to meet payment and other obligations | High |
| | | B33 | Scheme governance authority is subject to unexpected civil/criminal liability that brings the VC scheme to a halt | Med |
| | | B34 | E-wallet provider faces compensation claims from customers if functionality of wallet is compromised or fails to provide expected functionality | Med |

| | | ID | Risk description | Rank |
|---|---|---|---|---|
| C) Risks to financial integrity | Money laundering and terrorist financing | C01 | Criminals are able to launder proceeds of crime because they can deposit/transfer VCs anonymously | High |
| | | C02 | Criminals are able to launder proceeds of crime because they can deposit/transfer VCs globally, rapidly and irrevocably | High |
| | | C03 | Criminals/terrorists use the VC remittance systems and accounts for financing purposes | High |
| | | C04 | Criminals/terrorists disguise the origins of criminal proceeds, undermining the ability of enforcement to obtain evidence and recover criminal assets | High |
| | | C05 | Market participants are controlled by criminals, terrorists or related organisations | High |
| | Financial crime risks | C11 | Criminal uses VC exchanges to trade illegal commodities and abuse regulated financial sector at point of entry | High |
| | | C12 | Restorative justice of victims of crime is hindered by criminal using VCs to avoid seizure of assets, confiscation and financial sanctions | High |
| | | C13 | Criminal can use VCs for anonymous extortion | High |
| | | C14 | Criminal organisations can use VCs to settle internal or inter-organisational payments | Med |
| | | C15 | VCs make it more feasible for individuals to engage in criminal activity | High |
| | | C16 | Hacking of VC software, wallets or exchanges allows a criminal to implicate others in the criminal activities they commit | Me |
| | | C17 | Criminals, terrorist financiers and even entire jurisdictions are able to avoid seizure of assets, confiscation, embargos and financial sanctions (incl. those imposed by IGOs) | Med |
| | | C18 | Criminals are able to create a VC scheme | High |
| | | C19 | Tax evaders are able to obtain income in VCs, outside monitored FC payment systems | Med |
| D) Risks to payment systems in FCs | | D01 | Payment service providers (PSPs) that use FC and also provide VC services suffer losses due laws that render VC contracts illegal | Low |
| | | D02 | PSPs that use FC and also provide VC services fail due to liquidity exposures in their VC operations | Low |
| | | D03 | PSPs that offer VC payment services suffer loss of reputation when VC payments fail, because they gave the impression that VCs were regulated | Med |
| | | D04 | Businesses in the real economy suffer losses due to disruptions in financial markets that were caused by VC assets blocked, delayed, etc. | Low |
| E) Risks to regulatory authorities | Reputation risks | E01 | Regulators decide to regulate VCs but the chosen regulatory approach fails | Med |
| | | E02 | Regulators do not regulate VCs but the viability of regulated financial institutions is compromised as a result of their interaction with VCs | Med |
| | | E03 | Regulation and supervision of conventional financial activities is circumvented by unregulated 'shadow' activities that incur the same risks | Med |
| | Legal | E11 | Regulator is subject to litigation as a result of introducing regulation that renders pre-existing contracts illegal/unenforceable | Low |
| | Risks to competition objectives | E21 | Should the regulator decide to regulate VCs more leniently than FCs, an unequal playing field in the market for payment services will emerge | Med |
| | | E22 | If an unequal playing field is retained, the intensity of competition in the market for FC payment services diminishes as providers exit FC markets | Med |
| | | E23 | Regulators prevent potential new entrants to payment services market if the regulatory approach to VCs is excessive | Med |
| | To authority issuing FC (out of scope of | E31 | Should VCs gain widespread acceptance, central bank as issuer of FC can no longer steer the economy, as the impact of its monetary measures become difficult to predict | Low |

## Risks to users

68. VCs create numerous risks for users, and natural persons in particular. Some of these arise irrespective of the intended usage and purpose of holding or buying VCs, while others are specific to VCs used as a means of payment or as an investment.

### Risks that arise irrespective of intended usage

69. The user risks in this category exist because of the technology underlying VCs and their general features.

#### User suffers loss when an exchange acts fraudulently (A01)

70. This risk arises when the conduct of employees of an exchange falls short of reasonable expectations by consumers; the exchange is not legally incorporated in a jurisdiction and cannot therefore be subjected to regulatory requirements; the corporate governance responsibilities of the exchange's senior management are unclear; and/or its business activities are not subject to an independent audit. The priority of this risk is high.

#### User suffers loss when the exchange they interact with does not exchange VC against FC (A02)

71. The risk can arise because anyone can anonymously create (and subsequently change the functioning of) a VC scheme. Anyone can set up and call themselves an exchange, and exchanges may not necessarily be registered entities subject to licensing or authorisation requirements. The priority of this risk is high.

#### User experiences drop in value of VCs due to significant or unexpected exchange rate fluctuation (A03)

72. Several different drivers can create this risk, including that VC markets, and the price formation therein, are relatively opaque, and that the VC price formation on exchanges can easily be manipulated, including by a concerted effort of a small number of large VC holders. Denial of service attacks may prevent processing of transactions, which can further exacerbate the problem. Finally, in the case of decentralised VC, there is, by design, no central authority that could intervene to stabilise exchange rates. The priority of this risk is high.

#### User holding VCs may unexpectedly become liable to tax requirements (A04)

73. The legal and regulatory treatment of VCs is unclear and inconsistent, as is their tax treatment. The taxable event and geographic location of the taxable event may also be unclear. This may potentially lead authorities to treat VCs as property, forcing users to track and pay capital gains. The priority of this risk is medium.

### As a member of a VC mining pool, a user does not receive a fair share of mined VC units (A05)

74. The mining of VCs requires increased computing power over time, often exceeding that of a single computer. Users therefore have an incentive to mine VC units by pooling their computing capacity in a consortium. However, a fair distribution of the mined units (or the equivalent in converted FC) to which each member is entitled might be subject to manipulation by the mining pool owner. Similarly, members might be exposed to other forms of unequal treatment, due to a lack of transparency in business practices.

75. Any automated, IT-based distribution mechanism may, in turn, be subject to errors, fraud and hacking, as is the verification of transactions that mining initially requires. No refund rights exist either, through which disadvantaged users would otherwise be compensated, nor can an incorrect distribution of VC units be revoked, as VC transactions are irreversible by design. The priority of this risk is low.

### User suffers loss when buying VCs that do not have the VC features that the user expects (A06)

76. The inevitable lack of standards and definitions found in innovative products and services makes it difficult for users to gauge the features of a particular VC scheme. The units of the VC scheme bought may even transpire to be different from the expected scheme. The risk arises because anyone can anonymously create (and subsequently change the functioning of) a VC scheme, any computer file can be misrepresented as a VC and any scheme name can be given to that file, including the name of an existing, genuine VC. Once the user detects the misrepresentation, they will be unable to reverse their decision as VC transactions are not reversible, the counterparties are anonymous, no legal contracts exist, and no complaints procedures are in place. The risk is of medium priority.

### User's computing capacity is abused for the mining benefit of others (A07)

77. The mining and exchange of VCs is dependent on access to the internet and the processing power of personal computers (PCs), of which ever more is required over time to mine a VC unit. Both the internet and the PC have an unfavourable track record of protection against malware and other forms of hacking, making it feasible for a user's PC to be infiltrated and its computing capacity to be misused for the mining benefit of others. The priority of the risk is low.

### User suffers loss due to changes made to the VC protocol or other key components (A08)

78. The risk arises because anyone can anonymously create (and subsequently change the functioning of) a VC scheme. The software protocol that controls the VC scheme is not subject to any independent standards and can be changed once a majority of miners agree. These changes may accidently introduce errors, or miners may not necessarily act in good faith. The priority of the risk is high.

### User is not in a position to identify and assess the risks arising from using VCs (A09)

79. The decentralised and unregulated nature of VCs makes it difficult for users to access independent and objective information that would explain the risks arising from holding VCs. Some users may also have unfair information advantages, and the emergence of new VCs will affect the incumbents, and their prices, in unpredictable ways. The priority of the risk is low.

### User is in violation of applicable laws and regulation (A10)

80. The regulatory and legal treatment of VCs is unclear and authorities may change their views unexpectedly, at short notice, and the view may not be communicated sufficiently. The priority of the risks is medium.

### User suffers loss through e-wallet theft, hacking or soft/hardware malfunction (A11)

81. The risk arises because e-wallets are software that are stored on the user's computer or mobile devices. Those devices might suffer from malfunction as might the software itself. Furthermore, their encryption can be hacked, and unlike a conventional FC, this is possible from anywhere in the world. In many VC schemes, the e-wallet is stored unencrypted, making it an even easier target for hacking or theft. Furthermore, the user has no refund right after fraud because there are no safeguards in place, such as a deposit protection scheme for conventional accounts, and because lost or stolen coins cannot be distinguished from unused coins. The priority of the risk is high.

### User suffers loss when exchange is hacked (A12)

82. An exchange may temporarily hold users' VC units but can be hacked. A user may suffer losses because of insufficient security measures implemented by the exchange, because the VC units were held in a separate account, because no own funds are available that could be used to repay users, because the user has no refund rights and because the transaction cannot be reversed. The risk priority is high.

### User's identity may be stolen when providing identification credentials (A13)

83. Some VC schemes require users to identify themselves on the internet or at VC cash machines when buying/selling VCs, through passport scans, iris scans or finger printing. However, these identification measures are not subject to regulations or data protection laws, nor is the underlying IT software subject to safety standards. As a result, the user has no guarantee that the credentials they provided will be processed securely and only used for the intended purpose. Similar risks also arise for conventional payment transactions. The priority of the risk is high.

### Market participants suffer losses due to unexpected application of laws that render contracts illegal or unenforceable (A14)

84. Until governmental and regulatory authorities have formed an opinion on VCs, legal uncertainty remains over any contractual relationships that market participants may have forged. Once authorities have formed a view, these legal contracts may be rendered illegal or unenforceable. The priority of the risk is medium.

### Market participants suffer losses due to delays in the recovery of VC units or the freezing of VC positions (A15)

85. The risk arises due to the anonymity of (some) counterparties, the decentralised set-up of VC schemes, the fact that counterparties have insufficient own funds, and that VC markets become temporarily illiquid. The priority of the risk is high.

### Market participants suffer losses due to counterparties/intermediaries failing to meet contractual settlement obligations (A16)

86. The risk arises due to the anonymity of (some) counterparties, which can undermine the enforcement of any legal contracts that may exist, the lack of 'payment vs. payment' procedures, the lack of settlement finality, the decentralised set-up of VC schemes, the fact that counterparties have insufficient own funds, and that VC markets become temporarily illiquid. The priority of the risk is high.

### Market participants suffer losses of VC units held in custody by others (A17)

87. The risk arises because the custodian is insolvent, behaves negligently or fraudulently, lacks adequate governance arrangements to oversee transactions, fails to keep adequate records, or has inadequate own funds to repay creditors. Also, transactions are not reversible. The priority of the risk is medium.

### Market participants suffer losses through information inequality regarding other market participants (A18)

88. The anonymity of some market participants and the lack of technological accessibility for others facilitate information inequality and insider know-how that are benefit the former and are to the detriment of the latter. The priority of the risk is medium.

## Risks that arise when using VCs as a means of payment

### User suffers loss when counterparty fails to meet contractual payment or settlement obligations (A21)

89. The risk arises because anyone can anonymously create (and subsequently change the functioning of) a VC scheme, no legal contract exists between the counterparties that could be enforced, the counterparties are not known to one another due to their anonymity, the

counterparties have insufficient own funds to meet payment obligations, the payment service is not sufficiently reliable, the underlying IT security infrastructure is fragile, and no settlement finality exists. The priority of the risk is high.

### User experiences loss of FC units when using a VC cash machine (A22)

90. When exchanging VCs for FCs at a VC cash machine, users cannot guarantee that the VC or FC units will be correctly credited to their benefit. This is because VC cash machines are not subject to harmonised technical specifications, nor are they subject to licensing requirements, and, when error or fraud occurs, VC transactions are not reversible. No effective complaints or redress procedures are in place either. The priority of the risk is medium.

### User has no guarantee that VCs are accepted by merchants as a means of payment on a permanent basis (A23)

91. The risk arises because merchants are required to accept only legal tender in notes and coins, but they are not required to accept non-legal tender such as VCs. Furthermore, merchants may decide to vary the acceptance of alternative VCs over time, switching between various VC schemes. Merchants may also deem the overall costs and risks of VCs too high or too uncertain. The priority of the risk is high.

### User suffers loss when the VC payment they have made to purchase a good is incorrectly debited from their e-wallet (A24)

92. The risk arises because no authority oversees the settlement process: instead the process is based on trust. Furthermore, if an error is detected, the transaction is irreversible, e-wallets may be hacked to conceal the error and no effective complaints and redress procedures are in place. The priority of the risk is high.

### User is not able to convert VCs into FC, or not at a reasonable price (A25)

93. The risk can arise, for example, at an exchange where illiquid markets, low market depth, a lack of market makers and a non-fluid exchange can prevent arbitrageurs to operate and provide liquidity. More fundamentally, the risk can also arise because anyone can anonymously create (and subsequently change the functioning of) a VC scheme. The priority of the risk is high.

### User cannot access their VCs after losing password/keys to their e-wallet (A26)

94. Unlike losing the password to your bank account, credit card or debit card, no central administrative entity may exist that could re-issue passwords. Additionally, no identity is attached to the e-wallet through which ownership could be proven. E-wallets can be hacked and no effective complains or redress procedures are in place. Although dependent on the amount at stake, the risk is deemed to be of high priority.

### User cannot access their VCs on an exchange that is a going concern (A27)

95. The user may temporarily store their VC units on an exchange that is a 'going concern' i.e. is still functioning without an immediate threat of liquidation. However, they may find themselves unable to access them, because the exchange is not bound by any legal contract and is not subject to regulatory conduct and security requirements. The exchange can block the transfer of VC funds, FC funds or both, or may suffer from a lack of own funds. Furthermore, the transfers are not reversible. Although dependent on the amount at stake, the risk is of high priority.

### User cannot access their VCs on an exchange that has gone out of business (A28)

96. Once an exchange has gone out of business, i.e. no longer has the resources needed to operate, users suffer because the exchange may have held insufficient own funds to satisfy the demands of its VC creditors, and the VC units may not have been held in a separate account in their name, but in that of the exchange instead. Furthermore, the status of VC creditors during bankruptcy proceedings and unwinding is also unclear. Whatever the causal drivers, users will have no right to be compensated for losses, nor are they protected by a scheme similar to a deposit guarantee scheme for conventional bank accounts. The priority of the risk is high.

## Risks when using VCs as an investment

97. Individuals may use VCs not only as a means of payment for goods and services but also as an investment. The investment may take the form of holdings in VC units themselves or in investment products such as exchange traded funds (ETFs) or contracts for difference (CFD) that use VCs as an underlying asset. The risks arising from these activities are listed below.

### User suffers loss as a result of VC prices being manipulated (A41)

98. The risk arises because of the low depth of VC markets; the ability of concerted action, by a small number of large VC holders, to undermine price formation; the general opaqueness of VC markets; and the absence of any central authority that could intervene to stabilise price formation. The priority of the risk is high.

### User investing in regulated financial instruments using unregulated VCs as an underlying suffers unexpected loss (A42)

99. The risk arises because the lack of regulation of the underlying amplifies any risk taken on by purchasing the regulated investment product, such as a collective investment scheme (CIS), derivative or structured products. In addition, the investment products are highly complex, the returns are uncertain, and the underlying is opaque. The priority of the risk is medium.

### User is misled by unreliable exchange rate data (A43)

100. The risk arises because the trading, market activity, market making, settlement and clearing on exchanges across the world are not subject to independent standards that would usually ensure there are reliable and consistent exchange rates. Furthermore, price formation in VC markets is opaque and subject to manipulation, and the execution of buy and sell orders lacks transparency. The priority of the risk is medium.

### User suffers loss when investing in a fraudulent or Ponzi VC investment scheme (A44)

101. The risk arises because the individuals involved in the underlying asset can conceal their identity and are therefore not subject to any probity requirements, nor are they required to disclose the risks to which the investor is exposed, etc. Furthermore, the nature of VCs leaves investors more vulnerable to abuse by a Ponzi scheme based on VCs than other, regulated forms of investments. Finally, the user may have no access to redress schemes. The risk is of medium priority.

### User is exposed to significant price volatility within very short time frames (A45)

102. The risk arises because the trading, market activity, market making, settlement and clearing on exchanges across the world are not subject to independent standards that would usually ensure there are reliable and consistent exchange rates. Instead, the price of a unit of a particular VC scheme depends on the extent to which it is adopted and accepted as mainstream, which is uncertain. Furthermore, the market depth (i.e. the size of an order needed to move the market price by a given amount) is low, price formation in VC markets is opaque and subject to manipulation, and the execution of buy and sell orders lacks transparency. The priority of the risk is medium.

### User cannot execute the VC exchange order at the expected price (A46)

103. The risk arises because VC exchanges tend to be cash poor. As a result, investors may find it difficult to sell the VCs when they want to, so as to prevent a loss or to make a profit. Furthermore, the low market depth gives rise to an increased execution risk, (i.e. that the order is not executed at the price expected by the user).

## Risks to non-user market participants

104. Risks also arise to other, non-user market participants, such as exchanges, trade platforms, e-wallet service providers, merchants and others. Some of the risks apply to all participants, while others are specific to only one of them.

## Risks specific to exchanges

### Exchange is unable to fulfil payment obligations denominated in VCs or FCs (B11)

105. The risk affects the exchange and, consequently, also affects its creditors, because the exchange lacks adequate governance arrangements to oversee transactions, fails to keep adequate records, or possesses inadequate funds to repay creditors. Additionally, the particular VC that is being exchanged, and the underlying protocol that controls it, could be technologically faulty or compromised, or the IT environment at the exchange itself could lack reliability or security. If the problem occurs once the exchange has defaulted, the risk arises because of insufficient financial safeguards against default and inadequate business continuity arrangements. The priority of the risk is high.

### Exchange is not in control of its own operation (B12)

106. The risk affects exchanges and, consequently, also affects their creditors, because the exchange lacks adequate governance arrangements to oversee transactions, fails to keep adequate records, and operates within an IT environment that lacks safeguards against hacking and loss of control. The priority of the risk is medium.

### Exchange suffers loss if refund policies are abused to hedge currency exchange transactions (B13)

107. If the exchange offers refund policies for VC transactions as a way to mitigate against one or more of the above risks, it may suffer losses as a result of other market participants abusing the policy to hedge VC currency exchange rate risks. The risk arises because of the high exchange rate volatility, and a transaction potentially taking a long time to be completed. The priority of the risk is medium.

## Risks specific to merchants

### After accepting VCs for payment, the merchant is not reimbursed (B21)

108. The risk arises because of the 'double-spending problem': unlike FC that has a physical representation in coins and notes, VC units are only digital files. Therefore, the act of spending a VC unit does not remove its data from the ownership of the original holder.

109. Electronic payment systems in FC prevent double-spending by having a central authoritative source that follows rules for authorising each transaction. By design, no central authority exists in a VC scheme. To prevent double-spending, VC schemes tend to use a decentralised system with separate nodes that follow the same protocol. The authenticity of each transaction is verified by adding it to a transaction ledger, called the block chain, which is to ensure that the inputs for the transaction have not previously been spent.

110. However, there is no guarantee that a particular VC scheme uses this verification approach, nor is it certain that if this approach is used, it is completed securely and is not compromised,

for example through 'blocking' individual users from the VC network. The priority of the risk is medium.

### Unlike a FC, the merchant cannot be certain that they will be able to spend the VCs received (B22)

111. Once the merchant receives units that are denominated in a particular VC, there is no guarantee they will be able to spend them, for example, to pay invoices. VCs are not legal tender and therefore do not have to be accepted by other merchants, nor will the merchant be able to pay their tax liabilities in VCs. Acceptance of VCs depends entirely on the voluntary consent by other market participants, who may decide to vary the acceptance of alternative VCs over time, switching between various VC schemes. There is also no central authority that would act as a redeemer of last resort. The priority of the risk is medium.

### The merchant cannot be certain of the FC purchasing power of the VCs they have received (B23)

112. The exchange rate between VC and FC fluctuates significantly, often within very short periods of time, and often due to unpredictable events, such as technological innovations or platform seizures. The purchasing power of a VC unit regarding goods and services denominated in a FC is therefore difficult to predict and exposes the merchant to exchange rate fluctuations. The priority of the risk is medium.

### Merchant faces compensation claims from customers if transactions have been wrongly debited (B24)

113. E-wallet providers, exchanges, trade platforms and most other VC market participants are not regulated, and do not have a physical presence. Therefore, the VC scheme is not regulated either. Should an error emerge in a VC transaction, the aggrieved market participants may be left in a situation whereby the merchant is the only participant to whom a complaint and compensation claims could be addressed. More fundamentally, the risk arises because anyone can anonymously create, and subsequently change the functioning and core components of, a VC scheme. The priority of the risk is medium.

## Risks specific to miscellaneous non-user market participants

### E-wallet provider loses e-wallet provided to individuals (B31)

114. E-wallets are digital files and therefore are not only susceptible to hacking and other security breaches but, unlike conventional wallets, can be stolen from anywhere in the world. Furthermore, the digital nature of e-wallets generates significant economies of scale, which in turn facilitates large-scale theft through internet hacking. The priority of the risk is high.

### Administrator of a (centralised) VC fails to meet payment and other obligations (B32)

115. The risk arises to the administrator and, therefore, indirectly to its creditors. This is because an administrator of a centralised VC is in control of the VC scheme and its rules, but may change the rules, act without integrity, lack adequate and secure IT infrastructure and governance arrangements to oversee transactions, fail to keep adequate records, possess inadequate funds to repay creditors, or act with insufficient integrity (possibly leading to civil or criminal liability that leads to the discontinuation of the VC service). Should the risk materialise once the administrator has defaulted, the causal drivers are insufficient financial safeguards against default and inadequate business continuity arrangements. The priority of the risk is high.

### E-wallet provider faces compensation claims from customers if the functionality of wallet is compromised or fails to provide expected features (B33)

116. The risk arises because of negligence on the part of the e-wallet service provider, inadequate governance arrangements, insufficient recordkeeping and lack of operational capacity. Additionally, e-wallet providers are not necessarily subject to legally binding terms and conditions with the user who holds the e-wallet. The user may therefore be misled about the functionality of its features, suffer a loss and will then seek to claim compensation from the e-wallet provider. The priority of the risk is medium.

## Risks to financial integrity

117. Risks to financial integrity comprise risks of money laundering and terrorist financing, as well as financial crime. While the risks across these two categories are manifold, their causal drivers are often very similar and are primarily related to the anonymity and borderless nature of VCs, and the fact that anyone can create a VC, including criminals and terrorists.

### Money laundering and terrorist financing risks

### Criminals are able to launder proceeds of crime because they can deposit and transfer VCs anonymously (C01)

118. The risk arises because senders and recipients can carry out VC transactions on a peer-to-peer basis that do not require personal identification as there are no names attached to wallet addresses. Furthermore, there is no intermediary that could notify authorities of suspicious transactions. The priority of the risk is high.

### Criminals are able to launder proceeds of crime because they can deposit and transfer VCs globally, rapidly and irrevocably (C02)

119. The risk arises because, as a means of payment, VC schemes are not confined to, and are accepted across, jurisdictional borders. VC transactions require nothing more than internet access, the VC infrastructure is often spread across globe, making it difficult to intercept transactions, and VC transactions tend not to be reversible. The priority of the risk is high.

### Criminals or terrorists use the VC remittance systems and accounts for financing purposes (C03)

120. The risk arises because, as a means of payment, VC schemes are not confined to, and are accepted across, jurisdictional borders. VC transactions require nothing more than internet access, the VC infrastructure is often spread across globe, making it difficult to intercept transactions, and VC transactions tend not to be reversible. The priority of the risk is high.

### Criminals or terrorists disguise the origins of criminal proceeds, undermining the ability of enforcement authorities to obtain evidence and recover criminal assets (C04)

121. The risk arises because, as a means of payment, VC schemes are not confined to, and are accepted across, jurisdictional borders. VC transactions require nothing more than internet access, the VC infrastructure is often spread across globe, making it difficult to intercept transactions, and VC transactions tend not to be reversible. The priority of the risk is high..

### Market participants are controlled by criminals, terrorists or related organisations (C05)

122. The risk arises because market participants are often led by individuals who are not 'fit and proper'. The risk also arises because VC schemes are not confined to, and are accepted across, jurisdictional borders. VC transactions require nothing more than internet access, the VC infrastructure is often spread across globe, making it difficult to intercept transactions, and VC transactions tend not to be reversible. The priority of the risk is high.

## Risks of financial crime

### Criminals use VC exchanges to avoid regulated financial sector and trade in illegal commodities (C11)

123. The risk arises because senders and recipients can carry out VC transactions on a peer-to-peer basis that do not require personal identification, because there are no names attached to wallet addresses, and without the need for an intermediary that could be required to notify authorities of suspicious transactions.

124. In addition, as a means of payment, VC schemes are not confined to, and are accepted across, jurisdictional borders. VC transactions require nothing more than internet access, the VC infrastructure is often spread across globe, making it difficult to intercept transactions, and VC transactions tend not to be reversible. The priority of the risk is high.

### Restorative justice for victims of crime is hindered by criminals using VCs to avoid seizure of assets and confiscation (C12)

125. In addition to the previously mentioned drivers of anonymity and the possibility for global and rapid peer-to-peer transactions, the risk is also caused by the possibility that law enforcement authorities are unable to target individual entities, as VCs do not require an intermediary (with the possible exception of exchanges). The priority of the risk is high.

### Criminals can use VCs for anonymous extortion (C13)

126. The risk arises because senders and recipients can carry out VC transactions on a peer-to-peer basis that do not require personal identification, because there are no names attached to wallet addresses, and without the need for an intermediary that could be required to notify authorities of suspicious transactions.

127. In addition, as a means of payment, VC schemes are not confined to, and are accepted across, jurisdictional borders. VC transactions require nothing more than internet access, the VC infrastructure is often spread across globe, making it difficult to intercept transactions, and VC transactions tend not to be reversible. The priority of the risk is high.

### Criminal organisations can use VCs for settlement of internal or inter-organisational payment needs (C14)

128. In addition to the previously mentioned drivers of anonymity and the possibility for global and rapid peer-to-peer transactions, the risk is also created because no interaction is required with the regulated financial system and the transactions are not monitored. The priority of the risk is medium.

### VCs make it more feasible for individuals to engage in criminal activity (C15)

129. The anonymity of the creation (and subsequent changes to the function of VCs) combined with the easy access to VCs, the easy exchange between VCs and FCs, and the ability to avoid regulated financial systems makes it more feasible for individuals to engage in criminal activity, including the illicit purchase of goods and services and tax evasion. The priority of the risk is high.

### The hacking of VC software, wallets, or exchanges allows a criminal to implicate others in the criminal activities that criminal commits (C16)

130. Criminals tend to use any means available to cover their tracks. Insufficient safeguards against the hacking and the lack of control of e-wallet providers, exchanges, trade platform and VC protocols allows a criminal to steal internet identities and therefore implicate others in the criminal activities they commit. The priority of the risk is medium

### Jurisdictions are able to avoid seizure of assets and confiscation, as well as international embargos and financial sanctions (C17)

131. VC transactions are not recorded and are anonymous, global and irrevocable. Also, decentralised VC transactions are not dependent on entities on which financial sanctions and embargoes could be imposed. As a result, it is difficult for governments and international governmental organisations to enforce financial sanctions or embargos against other jurisdictions, for example to further humanitarian objectives. The priority of the risk is high.

### Criminals are able to create a VC scheme and use it for criminal purposes (C18)

132. Given the anonymity of the sender and the recipient of VC transactions, and of the inventor(s) of the VC scheme, criminals are able to create anonymously a VC scheme and 'pre-mine' a substantial share before the VC units are more widely released. As and when the currency has gained popularity and benefits from a higher exchange rate (which is potentially many years later), the criminals will possess substantial purchasing power, without ever needing to interact with FCs or to use an exchange. The priority of the risk is high.

### Tax evaders are able obtain income denominated in VCs, outside monitored FC payment systems (C19)

133. VC transactions are not recorded and are anonymous, global and irrevocable. Also, decentralised VC transactions are not dependent on entities on which financial regulations could be imposed. The priority of the risk is medium.

## Risks to payment systems and payment service providers in FCs

134. The risks listed in this category cover issues that may potentially arise as a result of possible interdependencies between payment systems denominated in FCs and those denominated in VCs.

### PSPs that use FC and also provide VC services suffer losses due to laws that render VC contracts illegal (D01)

135. Until governmental and regulatory authorities have reached an opinion on VCs, legal uncertainty remains over any contractual relationships that market participants may have forged. Once authorities have reached an opinion, these legal contracts may be rendered illegal or unenforceable, with associated impacts on the liquidity of the PSP. The priority of the risk is low.

### PSPs that provide services in FC as well as VC fail to meet their contractual obligations as payment system participants due to liquidity exposures in their VC operations (D02)

136. The risk arises because of the decentralised setup of the VC system, the anonymity of (some) counterparties, VC counterparties failing to hold sufficient VC units to settle transactions, VC exchange price changing rapidly and the price formation not being transparent. Furthermore, the liquidity management of the PSPs may be inadequate; the need for liquidity may intensify, as well as potential operational problems in linking FC and VC (e.g. settlement failure, outages, capacity, fraud and data loss). The priority of the risk is low.

### PSPs in FCs offering VC payment services suffer loss and reputational risk when providing unregulated VC services that subsequently fail to perform (D03)

137. This risk applies, in particular, to credit institutions that are also PSPs, as they may offer additional VC payment services to their existing banking customers, therefore implying that the product offered is also regulated. Should the VC services fail to perform as expected, the PSP risks its reputation and, possibly, suffers a financial risk too. The risk arises because PSPs

have a legitimate incentive to innovate and provide better value or lower costs offerings to consumers, and because consumers have trust in their banks and the products they offer. The priority of the risk is medium.

### The overall economy suffers losses due to disruptions in financial markets that were caused by VC transactions and assets that were blocked or delayed, etc. (D04)

138. The risk arises in a scenario where VCs have grown to be so important that their non-functioning leads to unexpected credit and liquidity exposures of PSPs in VCs, which in turn delays VC and FC transactions to the detriment of the genuine business of the overall economy. The priority of the risk is low.

## Risks to regulatory authorities

139. Regulators themselves incur risks regardless of whether or not they do anything at all, deliberately decide not to regulate or decide to regulate but the approach fails. The risks may be of a legal nature, of a reputational nature or because the activity undermines one or more of the regulator's objectives. Unlike the risks in the previous categories, the mitigation of the risks listed below is firmly in the hands of the regulators.

### Reputational risks

### Regulators decide to regulate VCs but the chosen regulatory approach fails (E01)

140. The risk can arise if the analysis of the risks and the identification of the regulatory response have been incomplete, if the regulatory approach was arbitraged by market participants acting from outside the regulator's jurisdiction, or if the regulatory measures chosen were not suitable to mitigate the risks. The priority of the risk is medium.

### Regulators do not regulate VCs but the viability of regulated financial institutions is compromised as a result of their interaction with VCs (E02)

141. The risk can arise if a decision not to regulate was made based on an incomplete analysis of the VC risks, or if the decision was insufficiently communicated to market participants. The priority of the risk is medium.

### Regulation and supervision of conventional financial activities is circumvented by unregulated 'shadow' activities that incur the same risks (E03)

142. VC schemes offer the same service and are subject to the same risks as traditional payment systems in conventional FC, but do so outside of (or in ways only loosely linked to) the traditional payment systems. The absence of the regulation of VC schemes therefore undermines the regulator's objective of ensuring well-functioning payment systems. The risk arises because compliance costs are significantly lower in VC markets, if not non-existent, providing an incentive for market participants to use the unregulated markets and save compliance costs. The priority of the risk is medium.

### Legal risks

Regulator is subject to litigation as a result of introducing regulation that renders pre-existing contracts illegal/unenforceable (E11).

143. Once regulatory authorities come to a view on their regulatory approach to VCs, existing contractual relationships that market participants may have forged may be rendered illegal, which in some cases may prompt market participants to consider litigation action against the regulator. The priority of the risk is low.

### Risks to competition objectives

Should the regulator decide to regulate VCs more leniently than FCs, an unequal playing field will emerge in the market for payment and financial services (E21)

144. If regulators decide to regulate different activities that have the same function and the same risk profile with a differing degree of intensity (for example in terms of governance, prudential and anti-money laundering requirements), then an unequal level playing field is created in the market. This risk arises as a result of an incomplete analysis of VC risks.. The priority of the risk is medium.

If an unequal playing field is retained, the intensity of competition in the market for FC payment and financial services diminishes as providers exit FC markets (E22)

145. The risk arises as a result of participants in the market for FC payment services exiting the FC market due to cost pressures arising from competition with less regulated VC actors. The priority of the risk is medium.

Regulators prevent potential new entrants to the market for payment services if the regulatory approach to VCs is excessive (E23)

146. The risk can arise if the regulator's analysis of the risks arising from VCs was incomplete or insufficient or the identification of suitable regulatory measures was faulty. The priority of the risk is medium.

# The proposed regulatory approach

## Summary of the key risk drivers

147. To understand how to mitigate the risks described in the previous chapter, the drivers of the risks need to be identified and addressed. Figure 2 lists the risk drivers that have been identified in chronological order.

Figure 2: Overview of risk drivers

| # | Driver of risks | Risk(s) for which the driver is relevant |
|---|---|---|
| a | **VC schemes can be created (and their functioning subsequently changed) by anyone, anonymously:** Anyone can anonymously create a VC and can subsequently make changes to the VC protocol or other core components if the required majority of (anonymous) miners agree. | A02, A06, A08, A21, A25, B31, C05, C15, |
| b | **Payer and payee are anonymous:** Transmitters and recipients of VCs interact on a person-to-person basis but remain anonymous. | A01, A03, A05, A06, A21, B01, B02, B03, B05, C01, C02, C03, C04, C05, C11, C12, C13, C14, C15, C17, C18, D01, D02, D03, E22, |
| c | **Global reach:** the internet-based nature of VC schemes does not respect national and, therefore, jurisdictional boundaries | C01, C02, C03, C04, C05, C11, C13, C17, |
| d | **Lack of probity:** exchange is neither audited nor subject to governance and probity standards, and is subject to misappropriation, fraud and seizure | A01, B23, C04, |
| e | **Not a legal person:** market participants are not incorporated as entities that could be subjected to standards | A01, A02, C12, C17, |
| f | **Opaque price formation:** price formation on exchanges is not transparent and is not subject to reliable standards, and exchange rates differ significantly between exchanges, which facilitates manipulation of exchanges | A03, A41, A43, A44, A45, A46, B23, D02, D03 |
| g | **No refunds or payment guarantee:** VC transactions are not reversible, so no refunds are issued for erroneous transactions | A05, A06, A08, A 21, A22, A24, A27, A28, A29, A 43, B04 |
| h | **Unclear regulation:** the regulatory treatment is unclear and creates uncertainty for market participants | A04,A10, B01, D01, E02,11, E22 |
| I | **Lack of definitions and standards**: the features of a product can be misrepresented because of a lack of definitions and standards | A06, A42, |
| j | **Inadequate IT safety:** the IT systems, infrastructure, transaction ledger, VC protocol and encryption are either insecure, subject to fraud and manipulation, and, in the case of the protocol, can be changed through a majority of minders | A07, A08, A11, A21, A22, A41, A42, B11, B12, B21, B31, C16, D01, |
| k | **Information is neither objective nor equally distributed:** limited availability of comprehensible, independent and objective information on VC activities. As a result, some market participants benefit from information inequality, e.g. on events that influence price formation | A09, A41, A42,B05, B06, D03 |
| l | **Insufficient funds or VC units:** market participants have insufficient funds to meet financial obligations or to compensate creditors in the case of bankruptcy | A21, A28, A29, A30, B04, B12, D01, D02, |
| m | **No separation of accounts**: VC units temporarily held at an exchange are often not segregated from the exchange, i.e. held in client accounts | A27, A30, |
| n | **No complaint process**: no effective channel for users to complain | A06, A22, A42, B24, B33, |
| o | **Lack of access to redress**: no access to redress, compensation or protection schemes | A22, A28, A30, A42, A44, |
| p | **Lack of corporate capacity and governance**: lack of skills, expertise, systems , controls, organisational structure and governance exercised by market participants | A45, B04, B11, B12, B32, B33, E21 |
| q | **No reporting:** lack of reporting requirements to any authority, e.g. of suspicious transactions | C01, C02, C03, C04, C11, C13, C14, C16 |
| r | **Interconnectedness to FC:** VC units and FC funds can be exchanged easily, therefore creating spill-over effects or risks from VC to FC systems | D02, D03, D04, B05, |
| s | **Not legal tender**: merchants are not legally required to accept a particular (or any) VC and can switch between different VC schemes | A23 |
| t | **No stabilising authority**: no authority that could provide exchange rate stability and/or act as the redeemer of last resort | A44, B22, |

149. These risk drivers would need to be addressed to mitigate the risks identified in the previous chapter. The section below specifies the regulatory measures that would need to be taken to achieve this task. It is clear that a regulatory response that addresses the risks comprehensively – in other words, addresses risks that are comparable to risks in existing financial services, such as payment services and electronic money – would, in aggregate, require a substantial, and in some aspects unprecedented and untested, body of regulation, as well as resources to enforce the regulation.

150. This would include requirements for the governance of VC schemes, the segregation of client accounts, capital requirements and many others, which in aggregate would amount to a comprehensive regulatory approach, as described in the section below. It would be for EU legislators to form a view on whether this approach can be established within the scope of any of the existing EU directives or regulations, or whether a separate legal initiative would need to be started.

151. However, the details of a regulatory approach will take time to develop, and the feasibility of some components is yet to be assessed. As long as there is no regime in place, the question exists of whether some of the more pressing risks identified can and need to be mitigated. To that end, an 'immediate regulatory response' is proposed in a separate section below.

## A potential regulatory approach for the long term

152. This section addresses each of the risk drivers separately and, in aggregate, specifies a potential comprehensive regulatory approach for the long term.

### Scheme governance authority

153. To address risk driver a) – i.e. that anyone, including criminals, can anonymously create a VC without being held responsible for any changes made to the VC protocol, or other core elements of the VC scheme by others at a later stage – the creation of an entity that is accountable to the regulator would need to be a mandatory requirement for a VC scheme to be regulated as a financial service and for it to be allowed to interact with existing regulated financial services.

154. The entity would be called the 'scheme governance authority', which is a non-governmental entity that establishes and governs the rules for the use of a particular VC scheme.[24] It is a legal person, and is responsible for maintaining the integrity of the central transaction ledger, the protocol, and any other core functional component of the scheme. The scheme governance authority would be required to comply with regulatory and supervisory requirements of various kinds to mitigate identified risks.

[24] The concept of governance authority is derived from the European Central Bank, *Harmonised oversight approach and oversight standards for payment instruments*, February 2009. There, the governance authority is described as being accountable for the overall functioning of the scheme that promotes the (initiation of the) payment instrument in question and for ensuring that all the actors involved comply with the scheme's rules. Moreover, it is responsible for ensuring the scheme's compliance with oversight standards.

155. A governance authority may, at first, appear incompatible with the conceptual origins of VCs as a decentralised scheme that does not require the involvement of a central bank or government. However, the mandatory creation of a scheme governance body does not imply that VC units have to be centrally issued. This function can remain decentralised and be run through, for example, a protocol and a transaction ledger. If it is true that the decentralised VC schemes are secure, it should be possible for market participants to establish themselves as scheme governance authorities. However, if a legal person is not able to exercise authority over market participants and is therefore unaccountable to a regulator for compliance purposes, it would be unreasonable to expect a regulator to guarantee integrity in their place. In the case of a centralised VC scheme, the issuer of the scheme arguably already controls the core elements of the scheme.

### Customer due diligence (CDD) requirements

156. The risk driver b), which concerns the anonymity of payers and payees could be addressed, at least within the EU, by requiring exchanges, and any other non-user market participants that interact with FC, to comply with CDD requirements. CDD requirements include the collection and verification of basic identity information; matching names against lists of known parties (such as 'politically exposed persons'); determining the customer's risk in terms of likeliness to commit money laundering, terrorist finance or identity theft; and monitoring a customer's transactions against their expected behaviour and recorded profile, as well as that of the customer's peers.

157. With transfers and exchanges of VC units (other than person-to-person transactions between wallets), information on the payer and the payee has to be exchanged with the relevant scheme governance authority. These transactions are then not only traceable but can also be linked to an individual's identity. KYC requirements would need to be imposed on exchanges, scheme governing authorities and potentially on some other market participants too.

### Fitness and probity standards

158. To address risk driver d) -- the lack of probity of individuals that take decisions with potentially harmful effects on other market participants -- fitness and probity standards would have to be imposed on individuals performing specified functions in a scheme governance body, an exchange, and other relevant market participants. These standards will require individuals to be competent and capable, honest, ethical, financially sound and to act with integrity.

### Mandatory incorporation

159. To ensure that market participants such as scheme governance authorities and exchanges can be held accountable for their actions (risk driver e)), they would be required to incorporate themselves in an EU Member State as a legal person that has standing to sue and be sued. Furthermore, a separation of the different risks of conventional FC and VC activities will be required

### Transparent price formation and requirements against market abuse

160. To address the risk drivers of opaque price formation and market abuse (risk driver f), exchanges would need to be subject to market abuse requirements to prevent insider dealing (when a person makes use of information unavailable to other investors for personal gain) and market manipulation (when a person knowingly gives out false or misleading information to influence the price of a share for personal gain).

161. Furthermore, every transaction would therefore be documented, so authorities can monitor the process of price creation. To that end, exchanges would need to be authorised and subject to reporting requirements.

### Authorisation and corporate governance

162. To address risk driver p), market participants such as scheme governance authorities and exchanges (and perhaps others) would need to be registered and authorised before beginning to provide VC services. An authorisation should only be granted to a legal person established in a Member State. The authorisation requirements would need to be tailored to address the risks specific to each type of market participants, such as accreditation of IT security with international standards certified by an independent third party and periodic assessments, to mitigate IT security vulnerabilities.

163. In addition, information on the identity of persons who ultimately own or control the legal entity would need to be provided, including evidence of their being fit and proper persons, and that they are capable to run these businesses.

### Capital requirements

164. To ensure that market participants have sufficient funds to meet financial obligations in VC as well as FC, to compensate creditors during bankruptcy (risk driver l), and to absorb losses and facilitate an orderly wind-down, capital requirements will need to be placed on those participants that hold VC units on behalf of others. The requirements should consist of a fixed as well as a variable component that increase with business volume. The capital should to be held in a FC.

### Separation of client accounts

165. To address risk driver m), market participants that hold VC units on behalf of others would be required to segregate their client VCs from their own VCs, complete periodic reconciliations of VC trading systems and VC stock held, and to keep appropriate records of reconciliations and transactions.

### Evidence of secure IT systems

166. Given the exclusively digital-based nature of VCs, the IT security of a VC scheme is of utmost importance. Scheme governance authorities would be required to document the way in

which they intend to guarantee the integrity of the transaction ledger, the protocol, the IT infrastructure and any other relevant components. Related requirements may also need to be placed on other market participants, such as exchanges and e-wallet providers. It will be a resource intensive task for regulators to check the adequacy of the systems and controls.

### Payment guarantee and refunds

167. In the case of an unauthorised VC transaction, market participants involved in the transfer of the funds are required to refund to the payer immediately the amount of the unauthorised payment transaction and, where applicable, to restore the debited VC account to the state it would have been in had the unauthorised VC transaction not taken place. This would address risk driver g) regarding the lack of refunds and payment guarantees. Additional financial compensation may be determined in accordance with the law applicable to any contract concluded between the payer and their payment service provider.

168. Market participants could potentially comply with this requirement in various ways, and the effectiveness of each approach would require further assessment. These include: (a) the merchant keeping a deposit amount with a proxy as a condition of using the service, (which is used by the proxy to 'reverse' transactions as required); (b) the proxy maintaining a wallet for the sole purpose of sending unbacked IOU documents acknowledging the debt to the merchant (to which it will forward the 'cleared payment' – the merchant sees a payment immediately but cannot spend the money until the payment 'clears'); or (c), the proxy indicates to the merchant that it has received a valid payment, and will forward the payment on to the merchant once the customer has indicated that the merchant has fulfilled their part of the transactions.

### Separation of VC schemes from conventional payment systems

169. Risk driver r) regarding the interconnectivity between VC and FC schemes should mainly be addressed by the mitigation measures in pre-existing oversight requirements for payment systems. However, complete mitigation can only be assured by requiring regulated financial institutions that decide to provide VC services to establish a separate entity for the VC-related business. This is to make sure that VC activities do not impair the financial soundness and settlement obligations of the regulated financial entity.

### Miscellaneous requirements

170. Risk driver l), regarding the lack of definitions and standards, could be addressed by regulators defining broader terms, and for the scheme governance authority to develop more specific standards, quality marks and definitions, and to make this party responsible for public information. Drivers n) and o) could be mitigated by requiring firms to set up complaints and redress schemes that are akin to those already in place for regulated VCs.

171. Drivers k) and q) regarding the lack of reporting requirements and resultant non-objective information could be addressed by requiring relevant market participants to submit specified

documents to regulators, including the results of their transaction monitoring, data on the amount and exchange rate applied to executed transactions, in addition to an obligation to report suspicious transactions. The data and information provided can be used to produce more objective and reliable information for market participants. Some market participants would also be required to disclose terms and conditions of their services to consumers.

### Clear and transparent regulation

172. The risk driver of unclear regulation (h) would be addressed implicitly once the other risk drivers have been addressed and regulatory requirements along the proposal above have been put in place. However, even in this scenario, continued warnings to the public are likely to be required to make them aware of those risks that remain deliberately unmitigated, such as VC not being legal tender (see below).

### A global regulatory approach

173. As expressed in risk driver c), the global, internet-based nature of VCs would require a regulatory approach to strive for an international, and ideally global, coordination, otherwise it will be difficult achieve a successful regulatory regime. In the absence of a global approach, national regulators will be required to issue continued warnings to potential users to make them aware of the risks of VC schemes that do not comply with the regulatory regime.

### Risks drivers that remain deliberately unaddressed

174. The last two risk drivers (s and t) remain deliberately unaddressed. Given that VCs are not issued by a public authority, there is arguably no reason why a government would want to assign legal tender status to a VC scheme that is beyond its control. There will also be no requirement to establish a central authority that could provide exchange rate stability and would act as the redeemer of last resort. However, it is conceivable that a scheme governance authority may decide to take on this additional role, and as a result, the VC scheme would no longer be decentralised. The risk drivers will therefore remain unmitigated, as will any risks that derive from them. Market participants will need to be repeatedly reminded about the continued existence of these risks even once VC schemes are subject to a regulatory regime.

## The immediate regulatory response for the short term

175. The comprehensive regulatory approach outlined above would be highly resource-intensive. Moreover, this approach may take considerable time to develop, fine-tune and implement, depending (amongst other things) on the development of the VC market. The question, then, is what should the regulatory and supervisory approach be in the meantime?

176. The risks identified in the previous chapter highlight the issues that arise for users, exchanges, wallet providers, conventional payment service providers and regulators, as well as the dangers to financial integrity more generally. Some of these risks are considered to be

of high importance, and some others have already materialised, through losses and theft of VCs, the bankruptcy of VC exchanges or large-scale money laundering and other criminal activity.

177. Until a comprehensive regulatory regime is developed, (if it is developed at all), only those risks can be mitigated that arise in the interaction between VC schemes and the regulated financial services sector (but not those that arise from activities within or between VC schemes). This would include risks of money laundering and financial crime, the risks to conventional payment systems, and some risks to individual users. To that end, the EBA recommends that national supervisory authorities discourage credit institutions, payment institutions, and e-money institutions from buying, holding or selling VCs, thereby 'shielding' regulated financial services from VCs.

178. The EBA also recommends that EU legislators consider declaring virtual currency exchanges as 'obliged entities' that must comply with anti-money laundering and counter terrorist financing requirements set out in the EU Anti Money Laundering Directive.

179. Furthermore, the EBA cautions against drawing similarities between existing payment and payment-related services and some VC-based services. The decentralised nature of many VC schemes, the fact that the functioning and rules of a VC scheme can be changed, and the absence of a redeemer of last resort means that VCs are not comparable to conventional payment or electronic money services. As a result, they give rise to risks that do not exist in these services. Declaring some actors as falling into the remit of a specific national or EU law may therefore lend credibility to these actors and, by implication, to VC schemes themselves that may not necessarily be warranted.

180. The immediate response specified above would 'shield' regulated financial services from VC schemes. As a result, the response would mitigate the risks arising from the interaction between VC schemes and regulated financial services, but it would not mitigate those risks that arise within, and between, VCs themselves.

181. Other things being equal, this immediate response will allow VC schemes to innovate and develop outside of the financial services sector, including the development of solutions that would satisfy regulatory demands of the kind specified above. The immediate response would also still allow financial institutions to maintain, for example, a current account relationship with businesses active in the field of VCs.

## Legal basis for this Opinion

182. One of the tasks of the EBA, in accordance with Article 9 of its founding regulation, is to monitor new and existing financial activities and to adopt guidelines and recommendations with a view to promoting the safety and soundness of markets and the convergence of

regulatory practice. [25] VCs are one of the activities it has been monitoring since September 2013 and on which it now issues this Opinion.

183. Furthermore, Article 1(3) mandates the EBA to act in the field of activities of credit institutions, financial conglomerates, investment firms, payment institutions and e-money institutions in relation to issues not directly covered in the Capital Requirements Directive, Payment Services Directive and the E-Money Directive, including matters of corporate governance, auditing and financial reporting, provided that EBA actions are necessary to ensure there is the effective and consistent application of those acts.

184. The EBA issues this Opinion to national supervisory authorities of credit institutions, payment service providers and electronic money institutions (in accordance with Article 29(1)(a) of the EBA Regulation) and to the EU Council, Commission and Parliament (in accordance with Article 34 of the EBA Regulation) as legislators in the European Union.

## The rationale for a consistent regulatory response across the EU

185. With regard to national supervisory authorities, the aim of the Opinion is to build a common supervisory culture and practice across the European Union, and ensure there are uniform procedures and consistent approaches throughout. These form part of the EBA's regulatory response by seeking to put in place appropriate supervisory (and, in the long term, regulatory) practices in relation to VCs, insofar as this falls within the competence of national authorities. Given that the regulatory environment for VCs is undeveloped, an EBA Opinion is an appropriate tool on which guidelines or recommendations could be built at a later stage, should a more comprehensive regime be developed in European Union law.

186. The European Parliament, Council and Commission can use the EBA Opinion to identify risks to consumers across the EU and to recommend that the EU institutions propose new legislation or amend existing legislation to establish those aspects of the regulatory regime proposed by the EBA that are not already established in European Union law.

187. The need for a regulatory response at European Union level by the EBA should be assessed against the EBA's objective, as established in Article 1(5) of the EBA Regulation, of protecting the public interest by contributing to the short-, medium- and long-term stability and effectiveness of the financial system, for the European Union economy, its citizens and businesses. In doing so, the EBA contributes to:

- improving the functioning of the internal market, including, in particular, a sound, effective and consistent level of regulation and supervision;
- ensuring the integrity, transparency, efficiency and orderly functioning of financial markets;
- strengthening international supervisory coordination;
- preventing regulatory arbitrage and promoting equal conditions of competition;

[25] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32010R1093&from=EN

- ensuring the taking of credit and other risks are appropriately regulated and supervised; and
- enhancing customer protection.

188. Where the EBA proposes legislative action by European Union institutions, it should take into account the powers available to the institutions to adopt legislation, and the principles of proportionality and subsidiarity. European Union financial services legislation is typically adopted either under Article 53(1) of the Treaty on the Functioning of the European Union (TFEU) (e.g. the Capital Requirements Directive), which concerns freedom of movement and the right of establishment, or Article 114 of the TFEU (e.g. the Capital Requirements Regulation), which concerns the approximation of law, regulation and administrative action with the object of the establishment and functioning of the internal market.

189. The EBA is therefore in a position to propose a regulatory regime to ensure that providers of VCs have access to the internal market regardless of the Member State in which they are established. A level of regulation can be established to ensure there is appropriate oversight in all Member States to support the wider access to the internal market. Legislation could establish minimum levels of regulation, a fully harmonised regime or a hybrid approach.

190. It is necessary for the EBA to establish whether this action should be taken at European Union level, i.e. whether the objectives of the regulatory response can be sufficiently achieved by the Member States or whether, by reason of the scale or effects of the proposed action, it can be better achieved at European Union level.

191. The clear advantage of action being taken at European Union level in respect of VCs is the possibility to implement a consistent level of regulation which ensures that the risks identified are mitigated for all market participants in the European Union. Without a Union response, national regimes are likely to take differing forms. The nature of VCs is that they can be provided from one Member State but used across the European Union (and beyond) with little or no local infrastructure needed. Differing levels or forms of regulation in one Member State could therefore lead to the VC industry shopping for the most convenient approach to the regulation, with European Union consumers receiving accordingly different levels of protection.

192. While only action at European Union level could ensure that providers of VCs can make use of the internal market, this may be a limited advantage given that while VCs may be used across national borders, there may only be limited cross-border provision of currency services or of cross-border establishments being used. Nevertheless, only regulation at European Union level can ensure there is removal or minimisation of any barriers to cross-border provision of services or cross-border establishments.