IMF STAFF DISCUSSION NOTE

Virtual Currencies and Beyond: Initial Considerations

Dong He, Karl Habermeier, Ross Leckow,

Vikram Haksar, Yasmin Almeida, Mikari Kashima,

Nadim Kyriakos-Saad, Hiroko Oura,

Tahsin Saadi Sedik, Natalia Stetsenko, and

Concepcion Verdugo-Yepes

INTERNATIONAL MONETARY FUND

Monetary and Capital Markets, Legal, and Strategy and Policy Review Departments

Virtual Currencies and Beyond: Initial Considerations

Prepared by an IMF Staff Team[1]

Authorized for distribution by
José Viñals, Ross Leckow, and Siddharth Tiwari

DISCLAIMER: Staff Discussion Notes (SDNs) showcase policy-related analysis and research being developed by IMF staff members and are published to elicit comments and to encourage debate. The views expressed in Staff Discussion Notes are those of the author(s) and do not necessarily represent the views of the IMF, its Executive Board, or IMF management.

CONTENTS

TABLE

ANNEX

EXECUTIVE SUMMARY

New technologies—supported by advances in encryption and network computing—are driving transformational change in the global economy, including in how goods, services and assets are exchanged. An important development in this process has been the emergence of virtual currencies (VCs). VC schemes are private sector systems that, in many cases, facilitate peer-to-peer exchange bypassing traditional central clearinghouses. VCs and their associated technologies (notably distributed ledgers based on blockchains) are rapidly evolving, and the future landscape is difficult to predict.

VCs offer many potential benefits, including greater speed and efficiency in making payments and transfers—particularly across borders—and ultimately promoting financial inclusion. The distributed ledger technology underlying some VC schemes—an innovative decentralized means of keeping track of transactions in a large network—offers potential benefits that go far beyond VCs themselves.

At the same time, VCs pose considerable risks as potential vehicles for money laundering, terrorist financing, tax evasion and fraud. While risks to the conduct of monetary policy seem less likely to arise at this stage given the very small scale of VCs, risks to financial stability may eventually emerge as the new technologies become more widely used.

The development of effective regulatory responses to VCs is still at an early stage. VCs are difficult to regulate as they cut across the responsibilities of different agencies at the national level, and operate on a global scale. Many are opaque and operate outside of the conventional financial system, making it difficult to monitor their operations.

Regulators have begun to address these challenges, with a variety of approaches across countries. Responses have included clarifying the applicability of existing legislation to VCs, issuing warnings to consumers, imposing licensing requirements on certain VC market participants, prohibiting financial institutions from dealing in VCs, completely banning the use of VCs, and prosecuting violators. These approaches represent an initial policy response to the challenges that VCs pose, but further development is needed. In particular, national authorities will need to calibrate regulation in a manner that appropriately addresses the risks without stifling innovation.

More could be done at the international level to facilitate the process of developing and refining policies at the national level. International bodies are playing an important role in identifying and discussing the risks posed by VCs and possible regulatory responses, and they should continue to do so. As experience is gained, international standards and best practices could be considered to provide guidance on the most appropriate regulatory responses in different fields, thereby promoting harmonization across jurisdictions. Such standards could also set out frameworks for cross-country cooperation and coordination in areas such as information sharing and the investigation and prosecution of cross-border offenses.

INTRODUCTION

A. Overview

1.   New technologies are driving transformational changes in the global economy, including in how goods, services, and assets are exchanged. The development of monies and a variety of payments systems throughout history have helped make exchange more efficient and secure. The rapid spread of Internet-based commerce and mobile technology—supported by advances in encryption and network computing—has driven the development of several innovative technologies. Companies such as Uber and Airbnb have developed radical new business models. Secure online payments systems (for example, PayPal) and mobile payments and transfer solutions (for example, M-Pesa) are changing the ways in which payments for goods and services are made.

2.   An important development in this process of transformation has been the emergence of virtual currencies (VCs). VCs, in principle, question the paradigm of state-supported fiat currencies and the dominant role that central banks and conventional financial institutions have played in the operation of the financial system. VCs are issued without the involvement or backing of a state. Some VC schemes make use of "distributed ledger" technologies that provide complete and secure transaction records without using a central registry. These technologies therefore allow for direct peer-to-peer transactions and eliminate the need for central clearinghouses. It is therefore not surprising that private sector interest in these new technologies has been growing, and that attention from regulators and policymakers has not been far behind.

3.   VCs and their underlying distributed ledger technologies have the potential to generate benefits. VC schemes and distributed ledger technologies can strengthen financial efficiency by facilitating peer-to-peer exchange while reducing transaction times and costs, especially across borders. In the longer term, these technologies have the potential to deepen financial inclusion by offering secure and lower-cost payments options. Beyond payments systems, distributed ledger technologies have implications for a wide range of markets and financial market infrastructures as a fast, accurate and secure record keeping system, including for stock exchanges, central securities depositories, securities settlement systems or trade repositories. Technological and regulatory progress will be needed to realize these potential benefits.

4.   However, these technologies also pose risks. VCs can be misused as vehicles for money laundering, terrorist financing, and tax evasion, and other forms of illicit activity. While risks to the conduct of monetary policy seem less likely to arise, risks to financial stability may eventually emerge as the new technologies come into more wide-spread use. Although the growing use of distributed ledger technologies outside of the context of VCs pose far fewer risks, it may over time pose a serious challenge to parts of the business model of the established financial system. VCs and distributed ledger technologies will thus continue to attract the attention of policymakers and regulators at both the national and international levels.

5.   **Any policy response to VCs will need to strike an appropriate balance between forcefully addressing risks and abuses while avoiding overregulation that could stifle innovation.** The initial focus should be on the most pressing concerns related to VCs—including financial integrity, consumer/investor protection, and tax evasion—while leaving less immediate risks (for example, financial stability, monetary policy) to a later stage. VCs combine many different properties of electronic payment systems, currencies, and commodities that span the responsibilities of several types of regulators at the national level. VCs operate in a virtual world that reaches across borders, increasing potential risks and creating opportunities for regulatory arbitrage. Effective policy coordination will therefore be required at the national and international levels.

6.   **This paper discusses the potential benefits and risks posed by VCs and how financial regulators could approach them.** The paper begins by explaining what VCs are, and how they work. It then examines key features and related developments in distributed ledger technologies underlying decentralized VCs, along with their potential use for financial development and financial inclusion. The paper subsequently discusses the policy and regulatory implications of VCs generally and concludes with a brief discussion of areas for future analysis.

7.   **As a starting point, it is important to note that the VC landscape is still new and rapidly changing.** It is therefore not possible to fully predict the future direction and importance of these evolving technologies or to identify specific longer-term policy responses. The paper is therefore intended as a first step and a platform for further research and analysis. Many of the questions it raises are left for future discussion.

B.   What are Virtual Currencies?

8.   **VCs are digital representations of value, issued by private developers and denominated in their own unit of account.**[2] VCs can be obtained, stored, accessed, and transacted electronically, and can be used for a variety of purposes, as long as the transacting parties agree to use them. The concept of VCs covers a wider array of "currencies," ranging from simple IOUs of issuers (such as Internet or mobile coupons and airline miles), VCs backed by assets such as gold,[3] and "cryptocurrencies" such as Bitcoin.

9.   **As digital representations of value, VCs fall within the broader category of digital currencies (Figure 1).** However, they differ from other digital currencies, such as e-money, which is a digital payment mechanism for (and denominated in) fiat currency. VCs, on the other hand, are not denominated in fiat currency and have their own unit of account.

---

[2] Given the fast evolving nature of the industry, a universal definition has yet to emerge and could quickly change as the VC ecosystem continues to transform.

[3] This type of VCs is backed by the combination of existing tangible assets or national currencies and the creditworthiness of the issuer.

Figure 1. Taxonomy of Virtual Currencies

Digitally represents value ← Digital currencies → Denominated in legal tender (for example, PayPal, e-money)

Not denominated in legal tender ← Virtual currencies

Convertible to real-world goods, services, money ← Convertible → Non-convertible (game coins)

No Central Authority ← Decentralized → Centralized (WebMoney)

Uses tech from cryptography to validate ← Cryptocurrencies → Hundreds of cryptocurrencies (Bitcoin, Ripple, Litecoin, Ethereum...)

Source: IMF staff.

10.   VC schemes comprise two key elements: (i) the digital representation of value or "currency" that can be transferred between parties; and (ii) the underlying payment and settlement mechanisms, including the distributed ledger system (see the section on distributed ledgers and Box 2).

11.   VC schemes have different levels of convertibility to real-world goods, services, national currencies, or other VCs. *Non-convertible VCs* (or closed schemes) operate exclusively within a self-contained virtual environment. Under these systems, the exchange of VCs with fiat currency (or other VCs) or its use in payments for goods and services outside of the virtual domain is significantly restricted. In contrast, *convertible VCs* (or open schemes) allow for the exchange of the VC with fiat currency (or other VCs) and for payments for goods and services in the real economy.[4] The level of contact between convertible VCs and the real economy is much greater than is the case in closed schemes.[5]

12.   VC schemes can operate through a centralized, decentralized, or hybrid model. The operation of VC schemes includes three components: (i) the issuance and redeemability of the VC; (ii) mechanisms to implement and enforce internal rules on the use and circulation of the currency; and (iii) the payment and settlement process. Each area of operation may be managed by a trusted central (and private) party or in a decentralized manner among participants. Hybrid schemes also

---

[4] An additional distinction is sometimes made between unidirectional flow and bidirectional flow of convertibility, with the former referring to VCs that can be obtained in exchange for fiat currency (or other VCs), but cannot be converted back to fiat currency (or other VCs)—the flow of convertibility being unidirectional (for example, Nintendo Points, some frequent-flyer programs air miles)—and the latter—where the flow of convertibility is bidirectional (for example, Bitcoin, Linden Dollar). See ECB (2012).

[5] It should be noted that convertible VCs may be subject to illiquid markets, limiting their *de facto* convertibility.

exist, where some functions are performed by a central authority, while others are distributed among market participants.[6]

13.   Decentralized VC schemes use techniques from cryptography for their operations—hence the "cryptocurrency" moniker:

- **In decentralized systems, there is no central party (for example, a central bank) administering the system or issuing VCs.** Rather, the central party is replaced by a framework of internal protocols that govern the operation of the system and allow the verification of transactions to be performed by the system participants themselves. As payments and transactions are made through the system, these participants (often referred to as "miners") are rewarded in newly minted "currency" for performing the payment processing function (referred to as "mining"). This approach serves two purposes: it introduces newly minted VCs into the system and enables the decentralized operation of the VC scheme. In contrast to fiat currency, a cryptocurrency does not represent a liability on anyone.

- **These systems may allow for the issuance of a limited or unlimited number of currency units.** Under most such systems (including Bitcoin), there is currently a limit on the number of currency units that may ultimately be issued. However, new systems are emerging that do not include such limits.

- **Most cryptocurrencies are "pseudo-anonymous"**—while cryptocurrency transactions are publicly recorded, users are known only by their VC "addresses," which cannot be traced back to users' real-world identity. As such, cryptocurrency transactions are more transparent than cash but more anonymous than other forms of online payment.

- **Cryptocurrencies challenge the standard concept of fiat currencies**. The value of existing fiat currencies is backed by the creditworthiness of the central bank and the government. Centrally issued VCs rely on the backing of the private issuer's credibility while the value of privately issued currencies (see Box 1 and the next section) have historically been supported by the private issuer's credibility and commodity reserves. In contrast, the value of cryptocurrencies does not have any backing from any source. They derive value solely from the expectation that others would also value and use them.

14.   VCs can be obtained in a variety of ways. Convertible VCs can typically be purchased or exchanged with fiat currency or other VCs, through a VC exchange, through a trade platform,[7] or directly with another VC holder. They can also be obtained in payment for goods or services. As noted above, decentralized VCs can be obtained by participating in the transaction validation

---

[6] For example, Ripple.

[7] Trade platforms provide a forum where buyers and sellers can offer and bid for VCs (akin to a market place).

process (for example, "mining"). VCs are typically stored in a "VC wallet," either directly through a VC wallet software application or through an intermediary—a VC wallet service provider.[8]

15.   Ancillary service providers have entered the market. Payment facilitators operate as intermediaries between consumers and merchants/retailers, converting VC payments into fiat currency and bearing the exchange rate risk of the transaction. In the case of cryptocurrencies, some service providers offer additional anonymizing services that further obfuscate the traceability of transactions.

ARE VIRTUAL CURRENCIES MONEY?

16.   Several questions arise when considering the role of VCs as money.[9] Do they satisfy the legal definition of money and fulfill all the economic roles of money (store of value, medium of exchange, and unit of account)? How do they compare to other privately-issued monies that existed historically? If they become more widely used, could (or should) these privately-issued currencies substitute for national currencies?

---

[8] VC wallets are used by VC holders to hold and transact in VCs. Cryptocurrencies are stored in digital wallet software associated with cryptographic keys: (i) "public keys," which are used to encrypt data and function akin to an account number; and (ii) "private keys", which are needed for decryption and which function akin to a password to access the cryptocurrencies or a signature to authenticate transactions. Where no intermediary is involved (for example, VC wallet service provider), the loss of a private key will in effect result in the loss of the VCs held in the VC wallet, as the owner of the wallet cannot access its content. VC wallets can be held online ("hot storage") or offline ("cold storage"). The latter is considered to afford greater protection against hacking and theft.

[9] "Money" could have different meanings depending on the context. VCs are comparable to banknotes, coins, and other liabilities of the issuer—the central bank in a modern monetary system. These are also called high-powered money, central bank liability, base money, or outside money. In contrast, money supply includes base money and liabilities (denominated in the national currency) created by banks and bank-like financial institutions (such as deposits and some money market fund shares—called inside money). Even in a system where the central bank has a monopoly right to issue base money, the bulk of the money supply could be provided in a decentralized manner by multiple financial institutions. These financial institutions could be regulated or unregulated (such as shadow banks and as in the "free banking" regime (Gorton, 1985). On the other hand, there is currently no known financial institution that provides inside money in VCs, and the VC monetary system consists only of high-powered money.

A. Perspectives from Theory and History

17.   Theory and history offer some guide-posts for considering these questions (Box 1):

- **Theory**. High inflation in the 1970s after the end of the Bretton Woods System renewed skepticism in some quarters over granting central banks monopoly power to issue nonconvertible fiat currency.[10] Friedman and Schwartz (1986) and Fischer (1986) reject Hayek's proposal to denationalize money (1976). Other researchers, however, continue to contemplate *laissez-faire* monetary regimes, and there has also been extensive theoretical work on the feasibility and optimality of privately issued money under monopoly or competition.[11]

- **History**. VCs are not the first example of currencies privately issued in a decentralized manner. While VCs are of course very different from national currencies, monetary systems and the legal concept of money have evolved substantially over time and will continue to change in the future. VCs should thus not be judged solely based on their current characteristics or on how they compare to current monetary regimes.

18.   A detailed comparison of the characteristics of VCs with existing and historical currencies sheds further light on these issues (Table 1). For the sake of specificity, Bitcoin is used as a representative example of a VC and compared to a home currency, a foreign currency, and a commodity asset based on current arrangements. Moreover, for a historical perspective, the table also includes key features of a commodity (gold bullion), a commodity currency (gold/silver coins), and a fiat currency convertible into gold and other commodities (the gold standard). The experiences during the U.S. Greenback era are also included, when the government-issued nonconvertible fiat currency "Greenbacks" and private banks were allowed to issue notes as currency. The monetary policy discussion in the policy challenges section assesses whether VCs could provide desirable monetary systems or not.

---

[10] Convertibility in this section refers to convertibility of fiat currencies to commodity reserves and international reserves, in the context of the gold standard or the Bretton Woods System, in contrast with the convertibility of VCs into national currencies as discussed in the earlier section.

[11] See, for example, King (1983), White (1984), Taub (1985), Selgin (1988), and Selgin and White (1994).

<div style="border:1px solid black; padding:10px;">

Box 1. Public and Private Provision of Money: History and Theory

Both history and economic theory broadly seem to support a monetary regime with public provision of currency over a competitive private system. The historical track record of containing inflation is mixed across both private and public systems. However, public systems appear to function better when there is a systemic liquidity shortage at the time of a financial crisis and the need arises for a lender-of-last-resort (LOLR).

Resilience against inflation

There are examples where currency was provided by multiple private banks without high inflation. In fact, many central banks in major advanced economies were first established as private banks, and their currencies did not have legal tender or monopoly status (Box Table). Also, notes issued by (multiple) national banks during the U.S. Greenback era did not have legal tender status but were traded at par with government issued notes (Calomiris, 1988).

Box Table. The Origins of Central Bank Powers

Country	Date founded	Monopoly over note issue	Notes made legal tender	State ownership
France	1800	1848	1878	1945
Germany	1875	1875	1909	1948
Japan	1882	1884	1885	NA
Italy	1893	1893	1893	NA
United Kingdom (England)	1694	1844	1833	1946
United States	1913	1913	1933	NA
Canada	1934	1935	1935	1938

Source: Redish (1993).

But systems were needed to curb the tendency to print too much money. During the U.S. Greenback era, when convertibility was temporarily suspended to finance the Civil War, note-issuing private banks were subject to various regulations. Their notes were printed by the government and backed 111 percent by government bonds held on deposit at the Treasury (reserve requirement), making them indirect obligations of the government. The aggregate amount of nationally chartered banks' notes was capped though the limit was later abolished. Moreover, their value was supported by the expectation to resume convertibility when the war was over (Calomiris, 1988). Without these systems, privately-provided nonconvertible fiat money often ended up being supplied in excess. Redish (1993) shows an example of nonconvertible notes with legal tender status issued by a French private bank in the late 18th century. Privately provided notes in late-19th century Japan led to inflation when their supply ballooned after banks suspended convertibility to gold.

The inflation performance of public moneys has been mixed. Before the collapse of the Bretton Woods System, international monetary regimes were largely anchored by gold and/or pegs to the pound Sterling and U.S. dollar standard (Bordo, 1981, and Redish, 1993) that were successful in anchoring inflation. Excess inflation happened even under commodity currency regimes (coins) for seignorage revenue. Medieval European monarchs—who had a monopoly right to mint coins or charge a fee for running a mint—often debased the currency by raising the unit of account value of a coin at the mint and reducing the precious metal content per coin. In a contemporary context, macro policy mismanagement has often led to high inflation and hyperinflation, as observed in many emerging and developing economies. Among major advanced economies, high inflation occurred in the 1970s following the end of the Bretton Woods System.

</div>

These experiences underpinned substantial discussions on tying central banks' hands again by returning to a rules-based framework including the gold standard (Friedman and Schwartz, 1986).

Lender-of-last-resort

Theory suggests that the private provision of money is not optimal when an economy may face system-wide liquidity shortages.

- The efficiency of competitive market equilibrium has been a key rationale cited by supporters of private provision of money (White, 1984, and Selgin, 1988). However, competitive equilibrium may not be optimal when the market is incomplete, or there is asymmetric information that could cause moral hazard (Mas-Colell, Winston, and Green, 1995). Such imperfections are typical in financial markets. Markets are also incomplete in the sense that not every risk is insurable among individuals, and everyone in the system could be hit by a large, negative, systemic shock.

- Many researchers have thus argued that public provision of money could improve economic welfare. Weiss (1980) shows the welfare-improving role of central bank money and active monetary policy as these facilitate inter-temporal smoothing in an overlapping generations framework. Diamond and Dybvig (1983) and Bryant (1980) show the effectiveness of public liquidity and deposit insurance in managing bank runs. Private provision of liquidity becomes insufficient and leads to a crisis without public outside money if a systemic shock hits the system, and contagion risks are imminent (Allen and Gale, 2000, Freixas, Parigi, Rochet, 2000, Holmstrom and Tirole, 1998, Tirole, 2008).[1]

History also seems to suggest that central banks in major economies often emerged in response to the need for a creditworthy institution to be the LOLR and manage bank runs (Goodhart, 1988, Redish, 1993, Gorton and Huang, 2006). In early history, large private banks acted as LOLR, but the need to handle bank runs more systematically eventually made them central banks or led to the establishment of new central banks. In the U.S., J.P Morgan pledged large sums of his own money and convinced other New York bankers to do the same to shore up the banking system in the 1907 financial crisis. The experience eventually led to the establishment of the Federal Reserve Board in 1913. As of late 18th century, the Bank of England (BOE) was a private bank, serving as the government's banker. The BOE notes gained legal tender status and monopoly issuance power, as the bank had strong credibility to be able to provide liquidity for other banks in distress. Similar development is also observed with other major central banks (Box Table). The global financial crisis provided a further reminder of the need for a credible LOLR.

_____

1/ The welfare implication may become less clear when the moral hazard costs from LOLR are incorporated in the analyses.

Feature	Bitcoin	USD (home currency)	Euro (foreign currency)	Commodity (bullion)	Commodity currency (coin)	Gold standard	U.S. Greenback Era (1861–78)
Table 1. Characteristics of Currencies: A Comparison							
Economic demand factors							
Intrinsic value	None	None	None	Yes	Yes	None	None
Claim to issuers?	No	Yes	Yes	No	No	Yes	Yes
Legal tender	No	Yes	No (in the U.S.)	na	na	Mixed	Yes (no) to public note (private)
Used as a medium of exchange	Small, but rising especially in online retail	Yes	Limited (in the U.S.) possibly more for cross-border trade	Yes	Yes	Yes	Yes
Used as unit of account	No	Yes	No (in the U.S.)	Yes	Yes	Yes	Yes (all notes shared "dollar" unit)
Used as store of value	Yes, subject to very high exchange rate risk and sudden confidence shock	Yes, subject to inflation risk	Yes, subject to foreign exchange risk	Yes, subject to commodity price risk/cycle.	Yes, subject to dilution of quality (inflation/devaluation)	Yes, subject to devaluation risk	Yes, subject to inflation risk
Supply structures							
Monopoly/decentralized	Decentralized	Monopoly	Monopoly	Decentralized	Mixed	Mixed	Decentralized
Supply source	Private	Public	Foreign public	Private/public mining	Mixed	Mixed	Public and private
Supply quantity	Inflexible	Flexible	Flexible	Inflexible	Inflexible	Inflexible	Flexible
Supply rule	Computer program	Rule-based (inflation target)	Rule-based (inflation target)	Opportunity cost for mining	Tied to commodity in bullion	Tied to commodity by reserve ratio	Private note subject to reserve requirement.
Supply rule change (by issuers) possible?	Yes with agreement of majority miners	Yes	Yes	No	Quality of minted coins can be diluted.	Reserve ratio can be changed and economized	No for private banks.
Cost of production	High (electricity consumption for computation)	Low	Low	Very high (mining)	Medium	Low	Low

Table 1. Characteristics of Currencies: A Comparison, cntd.							
Feature	**Bitcoin**	**USD (home currency)**	**Euro (foreign currency)**	**Commodity (bullion)**	**Commodity currency (coin)**	**Gold standard**	**US Greenback Era (1861-78)**
Macro-financial stability risks							
Risk of hyperinflation due to over-supply?	No for individual VCs	Possible (with policy mismanagement)	...	Limited	Possible (by diluting coin quality)	Possible (by ending convertibility)	Possible (if losing credibility to resume convertibility)
Risk of long-term hyperdeflation	High	Low	...	High	High	High	Low
Base money quantity changes to temporary shocks?	No (limited even with rule changes)	Yes	No (to US money demand shocks)	No	No	Somewhat (by changing reserve ratio subject to total holding of gold)	Yes
Can the issuer be lender of last resort with outside money?	No	Yes	Yes	No	No	Yes to some extent for credible issuer	Yes for public, harder for private (due to reserve requirement)

Sources: Bordo (1981), Calomiris (1988), Redish (1993), and IMF staff.

B. Legal Perspectives

19.   VCs fall short of the legal concept of currency or money. While there is no generally accepted legal definition of currency or money, the following may be noted:

- **The legal concept of currency is associated with the power of the sovereign to establish a legal framework providing for central issuance of banknotes and coins.** Currency refers to the unit of account and the medium of exchange denominated by reference to that unit of account, prescribed by law. In the strict sense, currency refers to the banknotes and coins that are issued by a central authority (for example, the central bank) that has the exclusive right to do so. Currencies are given the status of legal tender under the state's legal framework,[12] which generally entitles the debtor to discharge monetary obligations with the currency through its mandatory acceptance within the relevant jurisdiction. As such, the value and credibility of a sovereign currency are intrinsically linked with the ability of the state to support that currency.

- **The legal concept of money is also based on the power of the state to regulate the monetary system.** As a legal matter, the concept of money is broader than the concept of currency, and includes not only banknotes and coins but also certain types of assets or instruments that are readily convertible into such banknotes and coins (for example, demand deposits). While money can be created by private parties (for example, banks) as well as central banks, it must generally be denominated in a currency issued by a sovereign authority, and must be intended to serve as a generally accepted medium of exchange within that state (Procter 2012).

---

[12] It should be noted that the definition of legal tender varies slightly among jurisdictions. For example, in some countries, legal tender rules allow the debtor to make a valid "tender"—that is, to take the necessary steps to complete a payment—but there is no obligation on the side of the creditor to accept the tender. A creditor, however, would be barred from recovering the debt in court, if he has refused to accept a valid tender. On the other hand, in other countries, it is unlawful to refuse legal tender in payment. In light of the differences in the definition of legal tender in the euro area, the European Commission adopted a recommendation in 2010 that the concept of legal tender should rely on three main elements: (i) a mandatory acceptance of banknotes and coins; (ii) for their full face value; and (iii) with a power to discharge debt.

C. Economic Perspectives

20.   At present, VCs do not completely fulfill the three economic roles associated with money: [13]

- **High price volatility of VCs limits their ability to serve as a reliable store of value.** VCs are not liabilities of a state, and most VCs are not liabilities of private entities either. Their prices have been highly unstable (see Figure 2), with volatility that is typically much higher than for national currency pairs. Both prices and volatility appear to be unrelated to economic or financial factors, making them hard to hedge or forecast (Yermack, 2013).[14]

- **The current small size and limited acceptance network of VCs significantly restricts their use as a medium of exchange.** Without legal tender status, a VC is accepted only when two parties agree to use it. Despite the very rapid growth of VC-based payments, the number and volume of transactions in VCs remain small. Indeed, the current total market value of VCs is about US$7 billion. [15] By contrast, U.S. currency in circulation is US$1.4 trillion, while U.S. money supply (M2) is about US$12 trillion.

- **As of now, there is little evidence that VCs are used as an independent unit of account.** In other words, rather than being used to measure the value of goods and services directly, they instead represent the value in fiat currency based on the VC exchange rate. Retailers who accept payment in VCs will quote prices in fiat currency, with the price in VC based on the exchange rate at a particular point in time.[16]

---

[13] See Yermack (2013); Lo and Wang (2014); and Ali, Barrdear, Clews and Southgate (2014).

[14] Given the current very low level of acceptance and transaction volume of VCs and the evidence they are being "hoarded" (stored for speculative purposes) in some cases, as opposed to being used as an alternative medium of exchange, demand for VCs is mainly driven by expectations about their future use. If the market believes that VCs, or their embedded payment network, will become more widely adopted, this will be reflected in the price at which individuals are willing to buy and sell a particular VC. Changes in these expectations are reflected in VC prices.

[15] Furthermore, Bitcoin, which accounts for about 90 percent of decentralized VC market value (http://coinmarketcap.com, January 11, 2016), had a small daily transaction volume of about US$70 million in 2015 (https://blockchain.info), which is marginal compared to the largest global credit card providers.

[16] Given the high exchange rate risk, most retailers also immediately convert payments received in Bitcoin into fiat currencies.
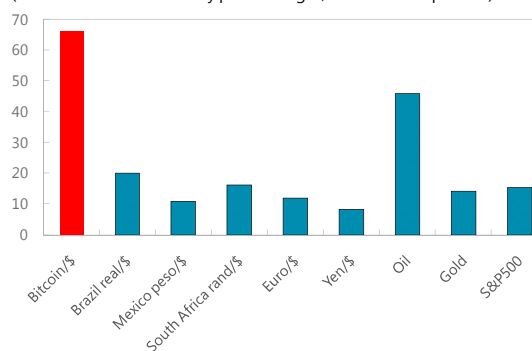
Figure 2. Volatility of Bitcoin Value

Bitcoins prices have been extremely volatility over the past several years...

...and more volatile than any other key currencies and assets.

The Value of Bitcoin
(U.S. dollar per bitcoin)

Volatility of Bitcoin and Selected Currencies and Assets, 2015
(Standard deviation of daily price changes, annualized in percent)

Sources: Coindesk.com, Datastream and IMF staff calculations.

DISTRIBUTED LEDGERS

A. What Are They and How Do They Work?

21. Exchange requires accounting, and modern payments systems are generally centralized (Figure 3). Typically, the central bank clears and settles payment requests from member financial institutions by moving money from one account on its central ledger to another. The member financial institutions will likewise adjust the positions of their individual members/account holders on their own internal ledgers. The central bank is responsible for validating transactions in its central ledger accurately and in a timely fashion to safeguard against double-spending or counterfeiting. The stability of the system depends on the trust vested in the central bank as an honest broker and its ability to safeguard the central ledger from tampering or failure.

22. Computing technology has made possible decentralized settlement systems built on *distributed ledgers* distributed across individual nodes in the payment system. Centralized systems have a master ledger keeping track of transactions maintained by a trusted central counter-party. In a distributed ledger system, multiple copies of the central ledger are maintained across the financial system network by a large number of individual private entities. The network's distributed ledgers—and hence individual transactions—are validated by using technologies derived from computing and cryptography, most often derived from the so-called blockchain technology. These technologies allow a consensus to be achieved across members of the network regarding the validity of the ledger.

23. This distributed ledger concept underpins decentralized VCs—for example the blockchain technology behind Bitcoin. The distributed ledger provides a complete history of transactions associated with the use of particular units of a decentralized VC. They provide a secure permanent record that cannot be manipulated by a single entity and do not require a central registry.

24.   Distributed ledger technologies have the potential to change finance by reducing costs and allowing for wider financial inclusion. In principle, they could be applied independently of a VC to any area that requires fast, accurate, and secure record keeping (for example, land and credit registries, and payment and settlement infrastructure for transactions in existing currencies, securities, and other assets).[17] In particular, it is possible to design distributed ledgers for transactions denominated in fiat currencies, instead of in VCs.

25.   There are various approaches to distributed ledgers, each with advantages and disadvantages (Box 2). The precise design chosen for a given application will depend on the needs of users, including mainstream financial institutions, infrastructures, and supervisors. Speed, efficiency, security, the level of trust in participants, and transparency (including for auditing and supervision) will be key factors in designing a given system and in defining the permissions that it requires. Some of the projects in which financial institutions are investing are based on existing platforms such as Bitcoin blockchain, Ripple or Ethereum. But momentum seems to be building for new technologies, many of them based on private blockchains. The following section provides further information.

---

[17] Reliable record keeping is a challenge even in well-developed institutional settings. For instance, even in the United States, the record of property title is imperfect. A buyer of a property usually hires a title search company to go through various records and confirm the seller and that only the seller has title to the property. In addition, buyers typically purchase title insurance in case somebody else claims ownership later. *The Economist* (2015a and 2015b) discusses ongoing effort of a country to use blockchain technology for improving its land registry.

Figure 3. Distributed Ledger System: How Does It Differ from Centralized Payment System?

A centralized payment system

Settlement accounts of banks at a central bank
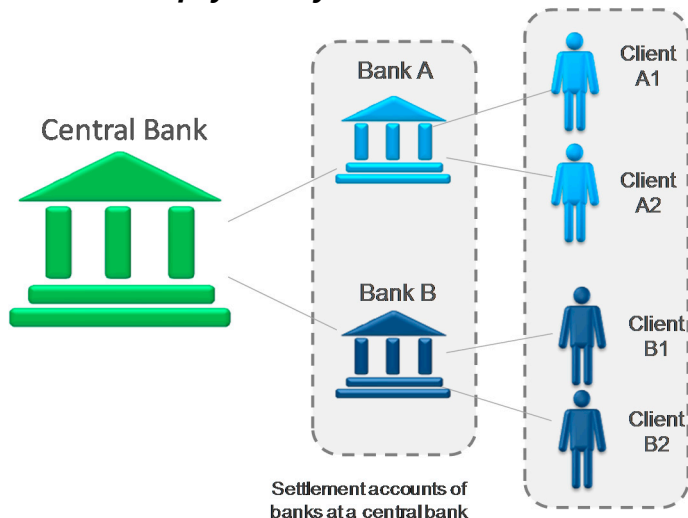
Payment from A1 to B1:

- Money is deducted from A1's account in bank A.
- The central bank moves money from bank A's settlement account to B's.
- The central bank maintains central record (ledger) of interbank transactions, by validating transactions and safeguarding against double-spending and counterfeit.
- Bank B adds money to B1's account.
- Banks A and B maintain the ledger of transactions for their clients A1 and B1 respectively.

*An illustrative example of distributed ledger system similar to Bitcoin (*Blockchain*)*
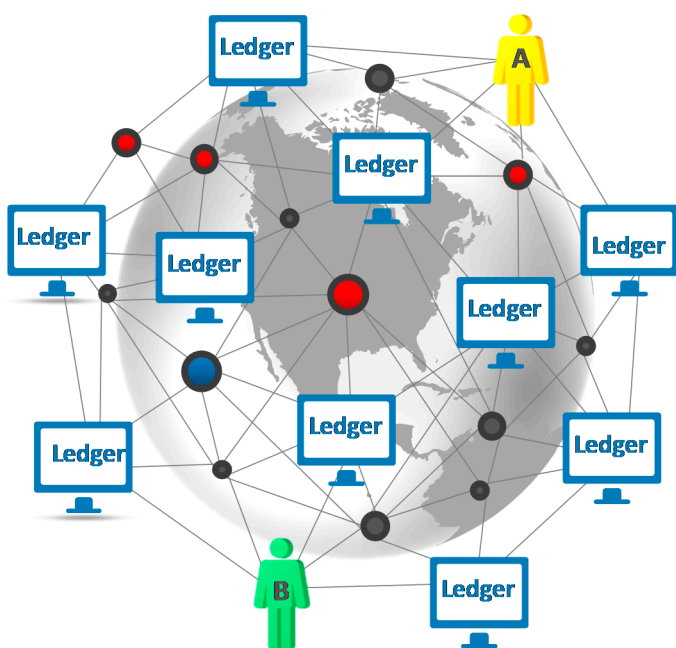
Payment from A to B:

- Copies of transaction records (ledgers) are kept in multiple computers in the network and visible to anyone.
- The transaction is settled by a multitude of individual nodes (miners), providing computing resources to the network.
- Miners solve a cryptographic puzzle as part of validation process. Miners need to show proof of doing this work to the network (called a "proof-of-work" system), which is costly (computing and energy resources).
- Only the miner who finds the solution faster than any others receives newly minted Bitcoins as reward for their service.
- "Trust" is created by making tampering attempts prohibitively expensive. If a miner wants to record a false transaction, she needs to compete against other miners who are acting honestly (or trying to fake a different transaction).[1]

1/ This mechanism could break down for example if a person or a group takes up 51 percent of the network (mining share), called a "51 percent attack." Some argue that strategic refinement could bring down this threshold to a much lower level (Garrat and Hayes, 2014). Even if a majority is required, the trust machine may break down if some of the miners gain a disproportionally large share of the system (for example, using military or state funds, Swanson, 2015).

Box 2. Design of Distributed Ledgers

There are various approaches to distributed ledgers, each with advantages and disadvantages (Buterin, 2015):

Fully public systems. These are decentralized ledgers open to all Internet users. Anyone can read, submit transactions, and participate in the verification and validation of transactions. The blockchains in these systems are secured by a combination of economic incentives and cryptographic verification, using mechanisms such as proof of work or proof of stake. Participants are typically known only by pseudonyms; and the issuance of an embedded currency provides incentives for participants to verify transactions and maintain the blockchain. Examples include, Bitcoin, Ethereum, and other cryptocurrencies.

Fully private systems. Permissions in these systems are assigned by a central entity. Applications include database management and auditing internal to a single company. A private system does not need an embedded currency given that the central entity can assign computers to verify transactions.

Hybrid or consortium systems. Here, the consensus validation process is controlled by pre-selected individuals or organizations, such as a consortium of financial institutions, or the customers of a company. The right to read the associated blockchain may be public or restricted to the participants. These systems are considered partially decentralized. The identity of users can be required to conform to know your business ("KYB") or know your customer ("KYC") procedures. Whether these systems need an embedded currency to provide incentives would depend on the degree of trust, which in turn would depend on the degree of decentralization.

B.   Emerging Uses of Distributed Ledgers

26.   Distributed ledger technology is already emerging in different parts of the mainstream financial system, including outside the context of VCs. Several startups, especially in the area of money transfer, offer blockchain-based platforms. Established financial institutions are also joining the competition. Some global banks have jointly started an initiative to develop distributed ledger technologies for use in global financial markets.[18] Some firms have launched blockchain-based security exchange platforms. Given that the industry is rapidly evolving, it is hard to gauge the full potential impact of these developments. But progress has already been made in several areas.

27.   Distributed ledger technology could reduce the cost of international transfers, especially remittances. The international transfer of funds is usually intermediated by correspondent banks. Through correspondent banking relationships—agreements between banks to provide payment services to each other—banks can access financial services in different jurisdictions and provide cross-border payment services to their customers. The costs of sending international remittances, however, are notoriously high: as of 2015, the global average cost of sending small

---

[18] For example, a consortium that includes most of the major global banks and is led by a U.S.-based firm (R3) is promoting collaboration and developing standards for blockchain applications in financial services http://r3cev.com/. More recently, the Linux Foundation announced a new collaborative effort to advance the use of blockchain technology. Many corporates, including major financial institutions, are participating in this initiative.

remittances (for example US$200) is 7.7 percent, though this has declined from just below 10 percent in 2008.[19] In contrast, the cost with Bitcoin is estimated to be about 1 percent (Goldman Sachs, 2014).[20] Recognizing the role of migrant remittances for home country growth and development, the G-20 has committed to reducing the costs of international remittances.[21] Indeed, a blockchain-based remittance system has already emerged in some economies. For instance, in the Philippines[22] and Kenya,[23] blockchain-based intermediaries offer money transfer services via Bitcoin and subsequent conversion of Bitcoins back into fiat currency for withdrawal by recipients through either their mobile phones or a bank account.

28.   **Distributed ledgers can shorten the time required to settle securities transactions.** Currently, settlement could take up to three days since trade date (called T+3) for most securities, including stocks, corporate bonds, municipal securities, and mutual funds shares. Many foreign exchange settlements continue to require two days (T+2).[24] Even U.S. Treasury bonds require at least one day (T+1). Not only is this time-consuming, but trading parties also face settlement and counterparty risks.[25] Major financial institutions have been investing substantially in this area. For example, Goldman Sachs applied for a patent on its blockchain-based settlement system (SETLCoin) in late 2015. The development of so-called smart contracts could further enhance the efficiency of transactions and settlements in the securities industry, but it also raises some risks (Box 3).

29.   **Relatedly, distributed ledger technologies can improve back office functions for securities dealers and enhance their transparency.** For example, in late 2015 NASDAQ, together with a blockchain startup, launched Linq, which is a blockchain-enabled exchange platform for

---

[19] World Bank, Remittance Prices Worldwide Database.

[20] However, the cost advantages of Bitcoin (and other VCs that adopts a similar "proof-of-work" system) may not be sustainable, as the cost of mining is expected to rise. Mining Bitcoin is costly, requiring computer processing power and associated energy costs. In addition, such systems involve a negative externality that causes overinvestment in computer power. The negative externality emerges because the expected marginal revenue of individual miners increases in the amount of computing power they individually use, but the difficulty of the puzzle they solve (marginal cost) increases in the total amount of computing power. Individual miners do not take into account the negative effect on other miners of their investment in computing resources. Therefore, all miners inefficiently overinvest in computer hardware, which results in significant waste of resources (Ali, Barrdear, Clews, and Southgate, 2014b). Moreover, seignorage for miners is set to decline over time, which may push miners to start charging more fees to users for compensation. Other VCs have adopted a "proof-of-stake" system to address this potential limitation (for example, Nextcoin). In a "proof-of-stake" system, instead of having miners compete to verify and validate the transaction, the transaction is assigned at random on the basis of the miner's "stake" in the network (that is, the number of coins he or she holds).

[21] The G-8 and G-20 endorsed pursuing the "5×5 objective," which aims to reduce the global average cost of sending remittances from about 10 percent in 2009 to 5 percent in five years.

[22] http://www.coindesk.com/new-phillipino-Bitcoin-exchsange-targets-remittance-market/

[23] http://www.theguardian.com/global-development/2014/aug/18/Bitcoin-remittances-market-digital-cash

[24] However, Continuous Linked Settlement (CLS) group, which settles a majority of global foreign exchange transactions, provides settlement finality in real-time.

[25] These risks arise if the counterparty defaults before settling an agreed trade. For example, the failure of Lehman Brothers caused a number of settlement fails in various markets.

privately-held companies. Linq facilitates the issuance, cataloging, and recording of transfers of these shares. The security issuers on Linq receive a comprehensive, historical record of issuance and transfer of their securities. Such a system could be applied to NASDAQ's public exchange as well. Moreover, some firms have started to issue bonds and equities digitally using blockchain technology, with approval from regulators.[26] Similar to Bitcoin, these securities could have a full history of change in ownership with a time stamp. Such detailed records, in principle, enhance the scope of accounting, auditing, and supervision, especially with the growing capacity to analyze big data.

Box 3. Smart Contracts

"Smart contracts" were first defined in the early 1990s as "a computerized protocol that executes the terms of a contract" (Szabo, 1994). A smart contract thus encodes the terms of a traditional contract into a computer program and executes them automatically.

With blockchain technology, smart contracts can in principle be self-executing and self-enforcing, without the need for intermediaries. They could encapsulate complex terms and conditions such as those found in many financial derivatives, which are often contingent on external events such as the prices of financial instruments or their volatility.

The potential benefits of using smart contracts are increased speed, efficiency, and trust that the contract will be executed as agreed. Smart contracts could overcome moral hazard problems (for example, strategic default) and reduce costs of verification and enforcement.

However, the legal status of these contracts is unclear and they could raise serious consumer protection issues. Widespread use of smart contracts could also increase risks to financial stability by automatically propagating adverse events through the financial system, with self-reinforcing feedback loops (similar to the risks posed by automated high-speed trading). The complexity of smart contracts may also make it hard for consumers to understand what they are agreeing to. Regulators and the court system may find it difficult to keep pace with these developments.

Blockchain-based smart contracts are still at an early stage, with many unsolved problems. Several platforms such as Ethereum and Codius seek to apply the blockchain technology to execute smart contracts. Unsolved technical difficulties include reliably observing and integrating external events. No viable smart contract systems have yet emerged.

---

30.   Together with other developments in financial technology, distributed ledger modalities could portend important structural shifts in the financial industry. Already, a growing number of blockchain-based financial services are being provided by non-bank startups, and some e-commerce firms are actively exploring the technology. At the same time, large global banks are also investing. Historically, large technological changes have led to significant adjustments in market shares, with new firms often gaining at the expense of established ones. At the very least, the internal structure and staffing of traditional financial intermediaries is likely to place an increasingly heavier weight on technology skills.

---

[26] http://www.wired.com/2015/12/sec-approves-plan-to-issue-company-stock-via-the-Bitcoin-blockchain/

REGULATORY AND POLICY CHALLENGES

31.   The potential for rapid change in the financial industry engendered by VCs is a challenge for financial regulators and supervisors. VCs are a relatively novel phenomenon and have emerged in the absence of effective regulation. This has contributed to their potential benefits, such as low transaction fees and processing time, but has left unaddressed the risks that VCs pose.[27] VC schemes pose risks to the financial system in a number of different areas. The risks are most serious with respect to cryptocurrencies but are not limited to them. Risks fall into a continuum, with immediate and pressing concerns about financial integrity (anti-money laundering/combating the financing of terrorism (AML/CFT)), consumer protection, tax evasion, and the regulation of capital movements. Concerns about financial stability, or the implications for monetary policy, are less immediate but will require further analysis and monitoring. The growing interest in blockchain technology, independent from a VC scheme, a priori raises fewer policy concerns, because the technology would be used in a closed system administered by regulated financial institutions.

A.   Regulatory Challenges and Responses

32.   The effective regulation of VCs poses, in some ways, unique challenges:

- **VCs pose a definitional challenge to regulators**. VCs combine properties of currencies, commodities, and payments systems, and their classification as one or the other will often have implications for their legal and regulatory treatment—in particular, in determining which national agencies should regulate them. Finding a consistent classification for VCs even within the same jurisdiction has proven difficult, as different competent authorities may classify them according to their own policy priorities. For example, the U.S. tax authority, the IRS, has classified VCs as "property" for the purpose of federal taxation,[28] whereas the Treasury Department's FinCEN has classified VCs as "value" for the purpose of AML/CFT obligations.[29] Other jurisdictions have taken a different approach, avoiding a formal classification and focusing instead on the nature or type of transaction being conducted. This disparity of treatment within and among jurisdictions may hamper coordination and may lead to inconsistencies.

- **VC schemes are difficult to monitor.** Their opaque nature makes it difficult to gather information, including statistical data, or to monitor their operation.

---

[27] The misuse of the technology has carried reputational costs for the industry and undermined consumer confidence, resulting in an internal push for self-regulation by some market participants, for example, The CryptoCurrency Certification Consortium (C4) and the CryptoCurrency Security Standard (CCSS) (Source: https://cryptoconsortium.org/about)

[28] https://www.irs.gov/pub/irs-drop/n-14-21.pdf

[29] https://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html

- **The transnational reach of VCs complicates regulation.** Asserting jurisdiction over a particular VC transaction, market participant, or scheme may prove challenging for national regulators in light of the cross-border reach of the technology.[30] National authorities may also find it difficult to enforce laws and regulations in a "virtual" (online) environment.

- **Cryptocurrencies pose particularly difficult challenges.** Their decentralized nature does not fit easily within traditional regulatory models. Through the use of distributed ledger technologies, cryptocurrencies eliminate the role of a central intermediary, such as an issuer or a payment processor, that would normally be the focal point of regulation. In such circumstances, the question then becomes who to regulate – for example, the individual VC users or other parties within the system.

33.   **Different regulatory responses have emerged to address the risks posed by this new technology, while reflecting the policy priorities of each jurisdiction.** The challenge for policymakers has often turned on finding a balance between addressing the risks and vulnerabilities posed by VCs while not stifling innovation. The responses have varied greatly among jurisdictions (see Annex). Some countries have decided to ban the use of VCs.[31] Other countries have addressed some of the immediate risks posed by VCs (financial integrity, tax evasion, consumer protection), in particular, by amending or clarifying the interpretations of existing laws and regulations,[32] or by issuing consumer warnings. A number of jurisdictions have yet to adopt a formal position on VCs.

34.   **In determining who to regulate, national authorities have mostly targeted VC market participants and financial institutions that interact with them.** While the issuance and transfer of VCs between users are less likely to pass through an intermediary, the interface between VCs and the broader economy—payments for goods and services and exchanges with fiat currency—will often go through a VC exchange or other VC service provider.[33] In addition, in light of the limited size of the VC network, it is generally accepted that VC users will have to "cash out" at some point—that is, convert their VCs into fiat currency. Recognizing these features of the current market, regulators have targeted "gatekeepers." In practice, this has been done in two ways: (i) by regulating VC market participants that provide an interface with the broader economy (for example, VC

---

[30] For example, the new regulation adopted by the New York Department of Financial Services (NYSDFS) makes the rules applicable to all entities who conduct Bitcoin businesses with New York residents, regardless of the VC market participant's location of business. See footnote 54.

[31] For example, Bolivia and Russia.

[32] For example, Canada amended existing laws in order to expand the coverage of AML/CFT requirements to VC businesses. The U.K. and U.S., among other countries, have clarified the tax treatment of VCs and the application of AML/CFT regulations to VC exchanges.

[33] It is worth noting that this is not necessarily the case. Fiat currency can be exchanged for VCs and vice versa on a peer-to-peer basis, and the same applies to goods or services. However, users will often choose to go through VC exchanges or other VC businesses for a variety of reasons (easier access, convenience, etc.).

exchanges); and/or (ii) by restricting the ability of regulated entities (for example, banks) to interact with VCs and VC market participants.[34]

35.   The effectiveness of emerging regulatory initiatives will depend on how the VC market evolves. While the approach of regulating VC "gatekeepers" is in line with the current characteristics of the market, a more widespread use of VCs may call for a more comprehensive regulatory response. For example, if the system becomes more operative purely on a peer-to-peer basis, regulating VC "gatekeepers" may not be enough. For this reason, a few regulators have gone further and are regulating a broader range of VC market participants (for example, VC wallet service providers) that operate entirely *within* the system. More broadly, the changing nature of the technology requires that regulation be flexible and can be adapted to evolving circumstances.

36.   Regulatory responses are also being developed at the international level. International efforts have focused on achieving consensus on the potential benefits and risks of VCs and identifying areas for future cooperation. A number of international bodies have both provided a forum to discuss issues related to VCs and contributed to the debate through the issuance of reports, guidance and manuals in their areas of expertise. In particular, the Financial Action Task Force (FATF)—the AML/CFT standard-setter—and the United Nations Office on Drugs and Crime (UNODC) have focused on the prevention and law enforcement response to the money laundering risks posed by VCs. The Committee on Payments and Market Infrastructures (CPMI) has considered the implications of VCs as a means of exchange and of distributed ledger technologies for central banks. Other institutions that have contributed to the debate include the OECD, the European Banking Authority (EBA), and the Commonwealth Secretariat.

37.   More could be done at the international level to facilitate the development of appropriate policy responses. As experience is gained, developing international standards and best practices could be considered to provide guidance on the most appropriate regulatory responses in different fields, thereby promoting harmonization across jurisdictions. [35] Such standards could also set out frameworks for cooperation and coordination across countries over such questions as the sharing of information and the investigation and prosecution of cross-border offenses.

38.   The following sections discuss in detail the specific risks posed by VCs in the areas of financial integrity, consumer protection, tax evasion and treatment, the enforcement of exchange controls, financial stability, and monetary policy.

---

[34] For example, the People's Bank of China has issued a notice to financial and payment institutions prohibiting their use of, or trade in, Bitcoin.

[35] The European Banking Authority (EBA) issued an opinion in July 2014 ("EBA Opinion on 'Virtual Currencies'") recommending that legislative action should be taken at the EU level in order to implement a consistent level of regulation among EU countries which ensures that the risks identified are mitigated for all market participants in the EU.

B. Financial Integrity: AML/CFT

39.   The anonymity and cross-border reach of VCs raise genuine concerns from a financial integrity standpoint. VCs can be used to conceal or disguise the illicit origin or sanctioned destination of funds, thus facilitating the money laundering (ML), terrorist financing (TF),[36] and the evasion of sanctions. Their traceability is limited due to user anonymity[37] and anonymizing service providers that obfuscate the transaction chain. These vulnerabilities are not only theoretical, but have been exploited in practice. VCs are often the "currency" of choice in cyber-related criminal activity. Bitcoin was, for example used in "Silk Road," a "dark web" market place for illegal goods that was shut down by U.S. law enforcement authorities in 2013.

40.   Applying AML/CFT controls to VC transactions can help prevent these abuses. Preventive measures—including customer due diligence (CDD) —transaction monitoring, and record keeping, and obligations to report suspicious transactions are an important component of national AML/CFT frameworks, and can assist in detecting, prosecuting and deterring instances of ML, predicate offenses, and TF. The challenge in applying AML/CFT controls to VCs is two-fold: (i) whether operations in VCs (for example, exchanges of VCs for fiat currency, transactions in VCs) should fall within the purview of the AML/CFT regime; and, if so, (ii) who should bear these obligations.

41.   The FATF, the international standard-setter for AML/CFT, has provided some guidance on the application of the AML/CFT standards to VCs.[38] The FATF has determined that the most significant ML/TF risks are concentrated in points of intersection between VCs and the regulated fiat currency financial system. As such, it has called for the regulation of VC exchanges and other network participants that operate as "gatekeepers" with the regulated fiat currency financial system. These would include currency exchanges in all types of VC schemes, but also the central authority within a centralized system if it performs currency exchange functions. As "*covered entities*" under the FATF standard, similarly to financial institutions, they would be required to implement preventive measures and report suspicious transactions. In contrast, the FATF has not advocated regulating parties that use VCs as a means of exchange to purchase goods or services.

42.   This approach reflects the current understanding of the ML/TF risks, but may eventually need to be extended to other VC network participants. If the use of VCs becomes so widespread that there is no longer a need for participants to "cash out" (that is, convert the VC into fiat currency), it may be necessary to extend regulation to other VC network participants such as wallet service providers and payment processors that operate entirely *within* the system. These

---

[36] There are several initiatives underway at the international and national levels to bolster the international CFT efforts which could have an impact on the use of new payment technologies, including VCs.

[37] Because of user anonymity, transactions recorded in the public ledger cannot be traced back to real world identities.

[38] FATF (2014 and 2015).

entities could be treated as *covered entities* and required to implement the preventive measures described above. Indeed the FATF standard would effectively require jurisdictions to consider additional mitigating measures if they determine that ML/TF risks cannot be contained by imposing AML/CFT controls on "gatekeepers" alone.

43.   Even with these changes however, enforcement will remain challenging.[39] This is particularly the case with decentralized VC schemes where law enforcement may not have a counterparty (for example, a central administrator) for investigative purposes and to implement freezing and seizing orders on funds held in VCs. In these circumstances, it is difficult to envisage how regulators could take enforcement actions, including the freezing of assets and the seizure and confiscation of illicit assets.

44.   While the issuance of guidance from FATF has helped clarify the appropriate responses to the ML/TF risks created by VCs, jurisdictions have taken different approaches to regulating them. Consistent with FATF's proposed approach, some jurisdictions (for example, U.S., Germany, U.K., Canada) have taken steps to clarify the applicability of existing AML/CFT obligations to certain virtual currency businesses, usually finding that VC administrators and exchanges do fall within *covered entities* for the purpose of AML/CFT preventive measures, while users usually do not. Some jurisdictions (for example, Italy) have taken a different approach by issuing advisories or warnings to their financial sectors on the ML/TF risks posed by VC businesses as customers, with some (for example, China) going as far as barring the interaction between VC businesses and the formal financial sector.

C. Consumer Protection

45.   The regulatory uncertainty and lack of transparency in VCs create significant consumer protection vulnerabilities:

- **Risks related to VC systems.** Disruptions to the VC systems can result in losses for the holders. These disruptions can be market-related or technology-related. For instance, a disruption in the VC protocol could paralyze the system.

- **Risks related to VC intermediaries and service providers.[40]** These include VC exchange platforms, VC wallet providers, payment processors, and brokers. Because many of these entities are for the most part unregulated, their customers are particularly vulnerable.

---

[39] Although VCs pose ML/TF risks, the distributed ledger technology itself may have benefits in combating ML/TF. Specifically, where it is adopted by financial institutions to decentralize know your customer requirements ("KYC") and AML/CFT registries, this technology could potentially make internal AML/CFT controls more cost effective, timely, and accurate.

[40] Mt. Gox, the largest Bitcoin exchange, filed for civil rehabilitation in Japan in February 2014, announcing that Bitcoins held for customers were missing. The company subsequently filed for liquidation proceedings in April 2014.

- **Risks related to scams—operations established with fraudulent intent.** Because of the opaque nature of the industry, the lack of regulatory safeguards and the complexity of the technology, VC holders are vulnerable to scams, such as stealing VCs (through hacking, fraud, false pretenses, or misrepresentations) to fraudulent investment schemes (which effectively operate as online Ponzi schemes). There have been some notable examples of VC exchanges and digital wallet providers being hacked, resulting in the theft of Bitcoins held for users.[41]

- **Risks related to the irreversibility of transactions.** Errors in transactions cannot be reversed.[42] Unlike credit cards, consumers have no right to reverse the charges if something goes wrong. As a related matter, a decentralized VC scheme places the risks associated with the failure of a transaction on the users of the system. This approach differs fundamentally from a centralized payment system where the central authority would assume this risk.

46.   Policy responses have aimed at increasing awareness of users and investors about these risks, and clarifying the scope of relevant legislation. For example, most countries have issued statements highlighting the above risks.[43] Jurisdictions are also beginning to clarify how existing consumer protection legislation (including securities legislation) applies to VCs or to amend such legislation where appropriate. National authorities have also taken enforcement actions against VC businesses found in violation of relevant legislation.[44]

While it was initially reported that the system was hacked by outsiders, the CEO of Mt. Gox was charged with embezzlement by Japanese prosecutors in September 2015.

[41] For example, Bitstamp, a large European Bitcoin exchange, suspended services in January 2015 due to a security breach involving the loss of 19,000 Bitcoin. Instawallet, a web-based wallet provider, also suspended services in April 2013 due to attack by hacking activities, resulting in the theft of over 35,000 Bitcoins (Congressional Research Service, 2015).

[42] Users cannot reclaim payment for erroneous transactions given that decentralized VCs lack a central intermediary as well as clarity regarding the counterpart.

[43] Some regulators have introduced, or are considering to introduce, regulations requiring registration to operate VC businesses, segregation of customer assets and/or posting of surety bonds to protect customers from the failure of VC intermediaries and service providers (e.g., New York, Connecticut, Japan—see footnote 54).

[44] In the U.S., the Securities Exchange Commission (SEC) filed a complaint against a company engaging in a Bitcoin-denominated Ponzi scheme pursuant to federal securities legislation which prohibit fraudulent offers and sales of "securities". The federal district court ruled that such Bitcoin-denominated investment vehicles should be considered as "securities" under federal securities legislation (SEC v. Shavers, E.D. Tex. August 6, 2013). In addition, SEC has taken enforcement actions against unregistered offerings of shares sold in exchange for Bitcoins (In the Matter of Erik T. Voorhees, Administrative Proceeding File No. 3-15902, June 3, 2014) and unregistered online VC-denominated stock exchanges and broker-dealers (In the Matter of BTC Trading, Corp. and Ethan Burnside, Administrative Proceeding File No. 3-16307, December 8, 2014 (Congressional Research Service (2015))). U.S. Commodity Futures Trading Commission (CFTC) has also taken enforcement actions pursuant to the Commodities Exchange Act against entities that operated an unregistered Bitcoin derivatives trading platform, ruling that Bitcoins and other VCs should be considered as "commodities" under the Act (In the Matter of Coinflip, Inc., d/b/a Derivabit, and Francisco Riordan, CFTC Docket No. 15-29, September 17, 2015).

D. Taxation

47.   VCs have a high potential as a means for tax evasion. This is particularly the case with cryptocurrencies, where participants need not disclose their identity, and transactions are peer-to-peer and can take place across borders. Given that tax evasion is already illegal in most jurisdictions, the key problems in this area relate to developing effective means of enforcement.

48.   To the extent that VCs are performing an economic function, whether as a store of value or a medium of exchange, they will have tax implications. The structure and operations of these schemes raise a number of complex issues related to the manner in which operations in VCs should be taxed. Although some major jurisdictions have made considerable strides toward resolving these issues, this is not the case in all countries.

49.   A key issue in the tax treatment of VCs is whether they should be treated as a form of (non-monetary) property, or as a form of currency.[45] Where the former position is adopted, use of a VC to purchase goods or services or for investment purposes would result in the recognition of gains or losses. The character of the gain or loss would depend on the applicable rules in the relevant jurisdiction, for example whether the property is defined to be a capital asset, the length of holding period, or the classification of a transaction as speculation. In the second case—when VCs are treated as a currency—most jurisdictions would require the recognition of foreign exchange gains or losses.

50.   Additional issues include the tax treatment of newly-created VCs obtained through mining (in the case of cryptocurrencies)—as opposed to acquiring already existing VCs—and the value-added tax (VAT) and sales tax treatment of transactions involving VCs. Country practices have varied significantly.[46] Further analysis and discussions are required—including legal and regulatory changes where needed—and greater international consistency should be promoted.

---

[45] Most countries that have addressed this issue have determined that VCs will be treated for income tax purposes as non-currency (or in a few cases non-domestic currency), property. See for example: U.S., IR-2014-36 and IRS Notice 2014-21 (March 25, 2014); Canada, CRA news release (May 11, 2013); U.K., Revenue and Customs Brief 09/14 (VCs are treated as foreign currency asset for income tax purposes); Australia, GSTR 2014/D3 (VC transactions are treated as if barter transactions, VC not money or foreign currency); France, declaration December 2013 (VCs cannot be legally considered a currency); Germany, 2014 (VCs are a form of "private money" treated like foreign exchange; earlier guidance suggested VCs are commodities, and therefore subject to taxation upon both sale of Bitcoin and sale of goods in exchange for Bitcoin).

[46]The first question is what kind of income is generated by mining. The U.S., for example, includes the fair market value at the time of mined currency in gross income (which also establishes the basis for any later disposition). Australia, by contrast, taxes miners only upon the sale or transfer of Bitcoins previously mined (which until then are treated as business inventory). Regarding the VAT and sales tax treatment of VCs, the U.K. (Revenue and Customs Brief 09/14) declared that: (i) use of VCs in purchase of any goods or services will be treated in the normal way for VAT, with the value being the sterling value of the VC at the time the transaction takes place; (ii) income from "mining" activities will be outside the scope of VAT; and (iii) exchange of VCs for British or foreign currency will not be subject to VAT on the value of the currency itself, nor on any fees or charges for arranging the transactions. Australia, in contrast, announced (ATO ruling GSTR 2014/D3) that Bitcoin exchanges and markets would have to charge GST on the full value of the Bitcoins they supply to residents, and not merely on any commissions charged.

51.   Tax record keeping requirements for VCs will be substantial and may reduce the attractiveness of VCs in everyday use. In many jurisdictions, such as the U.S., it will be necessary to calculate and report gains and losses on each use or disposition of Bitcoins. Use of a Bitcoin "agency" can facilitate this record keeping (at a price), but the taxpayer would still be responsible for accuracy. Multiple exchanges (for example for Bitcoin) with different prices further complicate record keeping. Guidance by the IRS in the U.S. so far prescribes only that the conversion to dollar-value must be "made in a reasonable manner consistently applied." Moreover, in the U.S., backup withholding will be applicable to payments made in Bitcoin, with payments in excess of $600 to a non-exempt person to be reported to both the IRS and the receiving person.

E.   Exchange Controls and Capital Flow Management

52.   VCs may also be used to circumvent exchange and capital controls. VCs can be used to effectively conduct a cross-border transfer of a fiat currency while bypassing traditional payment systems. As the applicability of national exchange control regimes to these systems is often unclear, the potential for VC schemes to serve as an avenue for the evasion of capital controls is obvious. This is particularly the case with decentralized schemes that combine speed, low transaction costs, and anonymity. The relative ease of acquiring VCs on the internet make them particularly attractive in regimes where the costs and national regulatory burden associated with traditional payment systems are high.

53.   There are already reports that VC schemes have been used to circumvent exchange and capital controls. Instances of evasion involving VCs have been reported in the media, notably in China, Venezuela, Cyprus, and Greece. Instead of purchasing foreign currency subject to government-imposed limitations, market participants can purchase VCs on the Internet and use them to conduct Internet-based foreign exchange transactions or make capital transfers that would otherwise be prohibited. The conversion of VCs can be done via peer-to-peer exchange floors or through marketplaces matching the sellers and buyers of VCs through complimentary purchases.[47]

F.   Financial Stability

54.   As of now, VCs do not pose systemic risks to financial stability, owing to their small scale and limited linkages to the financial system. VCs have still relatively limited market values and transaction volumes, relative to the mainstream financial system. The volume of transactions in decentralized VCs are marginal compared to the major credit card payments platforms, and do not yet amount to a systemically important payment network. Regulated financial institutions do not

---

Further, the *use* of Bitcoins would result in the application of two GSTs—one on the goods and services supplied in exchange, and one on the use of the Bitcoins themselves. In the U.S., New York has declared that transactions using Bitcoins will be treated as a barter transaction subject to sales tax.

[47] For example, the buyer of VC would purchase an online product for the seller of VC, who in turn would transfer to the buyer the corresponding amount in VC.

generally engage in VC-related activities, and VC-denominated derivatives[48] are still at the trial stage.

55.   VCs may pose non-negligible financial risks to individual VC holders and users. VC market infrastructures have suffered disruptions with some frequency, most notably the bankruptcy of the main Bitcoin exchange platform (Mt. Gox). However, no contagion to the wider financial system has thus far been observed. In addition, VC holders seem to engage in speculative hoarding,[49] with the potential for runs that could be triggered, for example, by a loss of confidence in the VC or in a particular third-party service provider such as a VC exchange. Runs are likely to be exacerbated by the absence of a LOLR function. In addition, like almost all IT systems, VCs are vulnerable to security breaches. Furthermore, VC users face payment system-like risks such as operational risk, credit risk, liquidity risk, and legal risk.[50]

56.   Large-scale use of VCs and greater interconnectedness with other parts of the financial sector could in due course give rise to systemic financial risks. In this case, the risks facing individual VC holders could spread to the broader financial sector. One significant source of risks may be the erosion of bank revenue from payments services.[51] Similarly, the potential widespread use of distributed ledger technology (for example, the blockchain) could have consequences for a wide range of markets and financial market infrastructures, including stock exchanges, central securities depositories, securities settlement systems, or trade repositories. Like most systems relying on cryptography, including traditional banking systems, VCs and blockchains are vulnerable to cryptographic risks.[52] This said, most of the potential channels of transmission are at this stage not clearly understood, and somewhat hypothetical in nature. Nonetheless, regulators and supervisors will want to closely analyze and monitor developments in these areas.

---

[48] See also footnote 44 for the treatment of VC-denominated derivatives pursuant to the Commodities Exchange Act in the U.S.

[49] Studies analyzing Bitcoin transaction patterns have, indeed found that a majority of all coins in circulation are being hoarded. See Ron and Shamir (2013), Meiklejohn et al (2013), and Badev and Chen (2014).

[50] For further discussion of these risks see ECB (2012 and 2015); Ali, Barrdear, Clews, and Southgate (2014a); and CPMI (2015). Credit and liquidity risks may occur for user funds held with third-party institutions that provide support for the use of VCs (for example, VC wallet service providers or exchange platforms) if there are no guarantees that these institutions can meet their obligations or provide liquidity to users when needed. Operational risk could occur if there is no sound operational procedure or business continuity plan. Legal risk arises from legal uncertainty regarding VCs.

[51] There is a risk that VCs could create an alternative payment system, subject to lower standards in terms of regulatory requirements. The uneven playing field may exacerbate the price advantage that VCs are able to offer their clients in addition to the technology advantages they enjoy. In the event VCs achieve scale, banks could lose a valuable source of revenue, which is also often an anchoring point for client relationships. Faced with a threat to revenue, banks may be forced to ramp up efforts to adopt and implement innovative technologies and business models to compete with VCs.

[52] Cryptographic systems depend on the assumption that an attacker would need a very long time to decrypt a message. However, this could change in the face of future advances in technology (for example, the development of quantum computers) or in mathematics (for example, new algorithms). See Dowd (2014).

57.   In addition, under a tail-risk scenario, some VC schemes or blockchains could become too big or too interconnected to fail, and could also be difficult to resolve. The difficulty would arise from a combination of factors: the use of strong encryption, a decentralized governance structure, and the cross-jurisdictional nature of VC networks. Monitoring rising systemic risks in this context would also pose additional challenges, given the anonymity of exposures and the lack of a governing regulatory framework.

58.   Regulatory responses to financial stability concerns are at their early stages. As of now, countries have generally taken the approach of limiting financial institutions' exposures to VCs by prohibiting them from engaging in VC businesses.[53] Some U.S. states have also introduced prudential regulatory frameworks for entities conducting "VC businesses" based on their rules regarding money transmitters.[54]

59.   The issues outlined above raise a number of questions for policymakers and regulators at both the national and international levels. At the national level, questions include (i) whether some VC intermediaries replicate the functions of a bank, which would require them to be regulated like a bank and (ii) whether VCs in VC-wallets should be considered as deposits protected by deposit insurance schemes. At the international level, given the cross-border nature of VC networks, a key question concerns who should oversee the VC markets and FMIs using the blockchain technology in payment, settlement, and other activities. While internationally agreed regulatory principles and cooperation among country authorities would be beneficial, the appropriate framework for such cooperation remains to be defined.

G.   Monetary Policy

60.   VCs do not currently have significant implications for monetary policy, but would raise some concerns if they become more widely used. VCs with rigid supply rules—the characteristics

---

[53] Some countries have more broadly prohibited financial institutions from using or trading in Bitcoin (for example, China—see Annex). The EBA's 2014 opinion (see footnote 35) also recommended national authorities in EU to discourage credit institutions, payment institutions, and e-money institutions from buying, holding or selling VCs, thereby "shielding" regulated financial services from VCs. The EBA notes that this immediate response will allow VC schemes to innovate and develop outside the financial services sector.

[54] In June 2015, New York Department of Financial Services (NYSDFS) issued regulations requiring businesses involved in transmitting, storing, buying, selling, exchanging, issuing, or administering VCs in New York to be licensed by the NYSDFS unless they are a state-chartered bank. The regulation requires licensees to be subject to minimum capital requirements, regulatory periodic examinations, financial disclosures, and approval of changes of control and mergers or acquisitions. Similarly, in June 2015, the Connecticut Money Transmission Act was amended to require licenses for all businesses engaged in the transmission of VCs in Connecticut. Under the revised Connecticut Transmission Act, such businesses are subject to all requirements applicable to money transmitters, as well as some additional requirements. Furthermore, the Conference of State Bank Supervisors developed a model framework for state VC regulatory regimes ("CSBS Model Regulatory Framework for State Regulation of Certain Virtual Currency Activities" (September 2015)). The Model Regulatory Framework notes that state regulators should ensure that the stability of the larger financial marketplace is maintained in allowing such activities, and recommends introducing financial strength requirements for VC companies, including capital and permissible investment standards, surety bond requirements, and development of policies for customer access to funds in the event of failure.

of many existing cryptocurrencies including Bitcoin—in principle have limited inflationary risk unlike many of the privately provided monies that existed in the past (see Table 1 and Box 2).[55] However, current VC systems lack other critical features that stable monetary regimes would typically be expected to provide. These include guarding against at least three key monetary stability risks: the risk of structural "deflation"; flexibility to respond to temporary shocks to money demand and thus smooth the business cycle; and the capacity to function as a LOLR.

61. **The nearly fixed supply of VCs—particularly many cryptocurrencies—could result in structural deflation in the same way as the gold standard.** Typically, money demand grows in line with the growth of the economy. When the supply of money is nearly fixed, continued money demand growth leads to structural deflation. Because of this, the gold standard and sterling or U.S. dollar based international reserve systems evolved to economize on limited reserves (Redish, 1993, and Bordo, 1981).[56] Modern monetary regimes with flexible money supply have a major advantage over VCs in this regard. However, in principle, VCs could be designed to allow an expansion in money supply, for example in line with transaction volumes, thus helping to overcome their deflationary bias in a growing economy.

62. **More generally, in an economy with a high share of VCs, the ability of monetary policy to manage the business cycle could be diminished.** Some of the challenges would be similar to those faced by countries that are heavily dollarized. The current generation of VCs does not allow for an expansion of the money supply in response to negative demand shocks. This would tend to exacerbate recessions and could lead to a deflationary spiral, as during the Great Depression under the gold standard.[57, 58]

63. **VCs will also not easily be able to replace the LOLR function of central banks.** The Global Financial Crisis again illustrated the importance of institutions that can provide emergency liquidity. Even with flexible supply rules, it is hard to see how a decentralized VC scheme could generate the type of liquidity response needed during a financial crisis. Experience and economic theory suggests that a public agency is needed to solve the externalities and coordination failures that arise in such cases (Box 1).

---

[55] However, Buiter (2014) points out that the proliferation of VCs and the expansion of the sum of all VCs may lead to inflation.

[56] The Fund's Special Drawing Rights (SDR) initially had a role of alleviating the structural shortages of international reserves.

[57] See, for example, Bordo, Choudhri, Schwartz (2002), Bernanke and James (1991), Temin (1989), and Eichengreen and Sachs (1985).

[58] It is unclear whether this limitation can be overcome by future generations of VCs. Notably, there is no obvious way to program VC supply rules to respond appropriately to all conceivable macroeconomic shocks. Even largely rule-based inflation-targeting regimes still require a great deal of judgment, especially in the face of large or qualitatively different shocks. Even substantially improved supply-rule programs that incorporate various contingency plans will probably not be flexible enough (Yellen, 2015; King, 2004), particularly in view of ongoing structural changes in the economy.

64.   **Absent regulatory measures and other interventions, VCs will likely be more widely adopted in countries with less credible monetary policy.** In general, the network benefits from using a single currency are substantial, and the costs of changing from one network to another would be large. These network externalities create a tendency toward having one dominant currency (the fiat currency) and confer a substantial incumbency advantage, which VCs could not easily overcome (Dowd, 2014). From this perspective, the appeal of VCs may be greater for countries where confidence in monetary policy is low, whereas a credible commitment to price stability will provide incentives to limit (or reduce) the use of VCs. However, the volatility of VC values has been so high that even for countries where confidence in monetary policy is low, dollarization may be a more attractive option than using VCs.

THE WAY FORWARD

65.   **This paper has been a first attempt by IMF staff to describe the principal features of VC schemes and their implications for regulation and policy.** The discussion set out above supports the following broad conclusions:

- VCs are rapidly evolving and the contours of the future landscape are difficult to predict.

- VCs offer many potential benefits, including rapidly increasing speed and efficiency in making payments and transfers, and deepening financial inclusion. The distributed ledger technology underlying some VC schemes offers benefits that go well beyond VCs themselves.

- At the same time, VCs pose many risks and threats to financial integrity, consumer protection, tax evasion, exchange control enforcement, and effective financial regulation. While risks to the conduct of monetary policy seem unlikely at this stage given VC's very small scale, it is possible that risks to financial stability may eventually emerge as new technologies come into more widespread use.

- The development of effective regulatory responses to the development of VCs is still at an early stage. Regulators in some areas (for example, AML/CFT) have made considerable progress in developing effective responses. However, a great deal of work remains to be done to put in place effective frameworks to regulate VCs in a manner that guards against the risks while not stifling financial and technological innovation.

66.   **The following principles could guide national authorities in further developing their regulatory responses:**

- **Regulatory responses should be commensurate to the risks without stifling innovation.** In this context, an outright ban may, in some cases, be unduly blunt while a more targeted approach (for example, regulating VC intermediaries) may be preferred.

- **Regulatory responses should adapt to the changes in the VC landscape.** Regulators should remain flexible in their approach so that challenges can be addressed as they arise.

- **Regulators should design approaches that take into account the novel business models inherent in VC schemes.** For example, in the absence of central authority in a cryptocurrency scheme that would normally be the subject of regulation, regulators need to focus on other VC market participants. Some countries are presently focusing on the "gatekeepers" (for example, VC exchanges) that serve as the bridge between a VC scheme and broader economy but this approach may need to be reconsidered if the VC market expands. In particular, other VC market participants that operate entirely *within* the network (for example, VC wallet providers) may eventually need to come under the regulatory framework.

- **Regulation may need to address not only market conduct issues (for example, AML/CFT, fraud), but also the financial soundness of VC intermediaries.** The failure of an intermediary may have implications for the protection of consumers and the stability of the payments system. Accordingly, regulators may need to consider imposing prudential regulatory requirements on VC intermediaries (as New York has already done).

- **Due consideration should be given to the degree of integration between the conventional financial system and the VC market.** Regulators should consider the potential implications of financial institutions (i) having VC intermediaries as clients; (ii) holding VCs as an investment; and (iii) performing the functions of VC intermediaries. In this context, regulators should consider whether to:
  - Prohibit any interaction between the financial institutions and the VC market;
  - Allow a certain degree of integration; or
  - Allow full integration.

67.   More can be done at the international level to help develop an effective international framework for the regulation of VCs:

- International bodies have a role to play in strengthening the international community's understanding of VCs more broadly. Several international bodies have already issued reports on VCs and have served as international fora for discussion (for example, the FATF, the Committee on Payments and Market Infrastructures in Basel, the European Commission, the European Central Bank, and the World Bank).

- More work is needed at the international level to study the evolution of VCs and their potential effects on the traditional banking and payments system, to understand the risks they pose, and to identify the most effective regulatory responses taking into account country circumstances.

68.   In the longer term and as experience is gained, consideration could be given to developing standards and best practices to provide guidance on the most appropriate regulatory responses to VC schemes in different fields. Some international standard-setting bodies have already initiated this process by providing guidance on the applicability of existing standards to VC schemes: FATF has issued guidance to member jurisdictions on the manner in which national AML/CFT frameworks should be applied to VC schemes under the FATF standard. Similar initiatives

could be explored for other international standard-setting bodies. Beyond clarification, the development of new principles may eventually become necessary. The establishment of international standards that take into account the specific features of VC schemes may promote harmonization in regulation across jurisdictions, and facilitate cooperation and coordination across countries over questions such as the sharing of information and the investigation and prosecution of cross-border offenses.

69.   An important process will need to involve ongoing monitoring and analysis of the manner in which VCs are evolving and the policy challenges that they pose. Many questions require further consideration. In particular, further work will be necessary in the following areas:

- How VC schemes and their underlying distributed ledger technologies will change existing business models in the financial sector, and what types of risk may arise from these developments.

- Whether the application of distributed ledger technologies in the mainstream financial system will evolve in a manner that gives rise to new specific risks that require a regulatory response.

- What potential implications VC schemes may have for the IMF now and in the future.

SELECTED BIBLIOGRAPHY

Ali, R., J. Barrdear, R. Clews, and J. Southgate, 2014a, "Innovations in Payment Technologies and the Emergence of Digital Currencies," Bank of England Quarterly Bulletin, vol 54, no 3, September, pp. 262–75.

_____, 2014b, "The Economics of Digital Currencies," Bank of England Quarterly Bulletin, Vol. 54, No. 3, pp. 276–86.

Allen, F. and D. Gale, 2000, "Financial Contagion," *Journal of Political Economy*. 108(1), pp.1–33.

Badev, A and M. Chen, 2014, "Bitcoin: Technical Background and Data Analysis," *Finance and Economics Discussion Series*, 2014–104, Board of Governors of the Federal Reserve System, December.

Bemanke, B. and H. James, 1991, "The Gold Standard, Deflation, and Financial Crisis in the Great Depression: An International Comparison," In *Financial Markets and Financial Crises*, University of Chicago Press, pp. 33–68.

Bordo, M. D. and F.E. Kydland, 1995, "The Gold Standard as a Rule: An Essay in Exploration," *Explorations in Economic History*, 32(4), pp. 423–464.

Bordo, M.D., 1981, "The Classical Gold Standard: Some Lessons for Today," *Federal Reserve Bank of St. Louis Review*, (May), pp. 2–17.

Bryant, J., 1980, "A Model of Reserves, Bank Runs, and Deposit Insurance," *Journal of Banking & Finance*, 4(4), pp. 335–344.

Buiter, W., 2014, "Gold: A Six Thousand Year-Old Bubble Revisited," *Global Economics View*, Citi Research.

Buterin V., 2015, "On Public and Private Blockchains," August 7.

Calomiris, C.W., 1988, "Price and Exchange Rate Determination During the Greenback Suspension," *Oxford Economic Papers*, pp.719–750.

Committee on Payments and Market Infrastructures (CPMI), 2015, *"Digital Currencies,"* November 2015, Bank for International Settlements (BIS).

Congressional Research Service, 2015, "Bitcoin: Questions, Answers, and Analysis of Legal Issues"

Diamond, D.W. and P.H. Dybvig, 1983, "Bank Runs, Deposit Insurance, and Liquidity," *The Journal of Political Economy*: 401–419.

Dowd, K., 2014, "New Private Monies: A Bit-Part Player?" Institute of Economic Affairs, Cobden Centre Hobart Paper No. 174. London: Institute of Economic Affairs.

Eichengreen, B. and J. Sachs, 1985, "Exchange Rates and Economic Recovery in the 1930s." *The Journal of Economic History*, 45(04), pp. 925–946.

European Central Bank, 2012, *Virtual Currency Schemes*, October (Germany).

_____, 2015, "Virtual Currency Schemes–A Further Analysis," February (Germany).

European Banking Authority, 2014, "EBA Opinion on 'Virtual Currencies*,"* EBA/Op/2014/08.

FATF, 2014, "VCs: Key Definitions and Potential AML/CFT Risk," June.

FATF, 2015,"Guidance for a Risk-Based Approach: Virtual Currencies" June.

Fischer, S., 1986, "Friedman Versus Hayek on Private Money: Review Essay," *Journal of Monetary Economics*: 17 (3), (May 1986), 433–440.

Freixas, X., B.M. Parigi, and J.C. Rochet, 2000, "Systemic Risk, Interbank Relations, and Liquidity Provision by the Central Bank," *Journal of Money, Credit and Banking*: pp. 611–638.

Friedman, M. and A.J. Schwartz, 1986, "Has Government any Role in Money?" *Journal of Monetary Economics*: 17(1), pp. 37–62.

Garratt R. and R. Hayes, 2014, "Bitcoin: How Likely is a 51 Percent Attack?" Liberty Street Economics, Federal Reserve Bank of New York, November 24.

Goodhart, C., 1988, "The Evolution of Central Banks," MIT Press Books, 1.

Goldman Sachs, 2014, "All About Bitcoin," Global Macro Research Top of Mind, March 11, 2014.

Gorton, G., 1985, "Banking Theory and Free Banking History: A Review Essay," *Journal of Monetary Economics*. 16(2), pp. 267–276.

Gorton, G. and L. Huang, 2006, "Bank Panics and the Endogeneity of Central Banking," *Journal of Monetary Economics*: 53(7), pp. 1613–1629.

Hayek, F.A., 1976, Denationalization of Money (London: Institute of Economic Affairs).

HM Treasury, "Digital Currencies: Response to the Call for Information," March 2015.

Holmstrom, B. and J. Tirole, 1998, "Private and Public Supply of Liquidity." *Journal of Political Economy*. 106 (1), pp. 1–40.

King, R.G., 1983, "On the Economics of Private Money," Journal of Monetary Economics, 12(1), pp. 127–158.

King, M., 2004, "The Institutions of Monetary Policy," NBER Working Paper 10400.

Lo, S. and J.C. Wang, 2014, "Bitcoin as Money?" Federal Reserve Bank of Boston, Current Policy Perspectives No 14–4, 2014, 14.

Mas-Colell, A., M.D. Whinston, and J.R. Green, 1995, Microeconomic Theory (Vol. 1). New York: Oxford University Press.

Meiklejohn, S., M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, 2013, "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names," Usenix, December 2013. Volume 38, Number 6.

Moore, T. and N. Christin, 2013, "Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk," in Financial Cryptography and Data Security.

Nakamoto, S., 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System," unpublished manuscript.

Procter, C., 2012, "Mann's Legal Aspect of Money," Oxford University Press.

Redish, A., 1993, "Anchors Aweigh: The Transition from Commodity Money to Fiat Money in Western Economies," *Canadian Journal of Economics*: pp. 777–795.

Ron, D. and A. Shamir, 2013, "Quantitative Analysis of the Full Bitcoin Transaction Graph," In *Proceedings of Financial Cryptography*, 2013.

Selgin, G.A., 1988, The Theory of Free Banking: Money Supply Under Competitive Note Issue, Rowman & Littlefield Pub., Inc.

_____, 2015, "Synthetic Commodity Money," *Journal of Financial Stability*, *17*, pp. 92–99.

Selgin, G.A. and L.H. White, 1994, "How Would the Invisible Hand Handle Money?" *Journal of Economic Literature*: pp. 1718–1749.

Smith, B.D. and W.E. Weber, 1999, "Private Money Creation and the Suffolk Banking System," *Journal of Money, Credit and Banking*: pp. 624–659.

Swanson, T., 2015, "Consensus-as-a-Service: A Brief Report on the Emergence of Permissioned, Distributed Ledger Systems," R3 CEV.

Szabo, N., 1994, "Smart Contracts," unpublished manuscript.

Taub, B., 1985, "Private Fiat Money with Many Suppliers," *Journal of Monetary Economics*, 16(2), pp. 195–208.

Temin, P., 1991, "Lessons from the Great Depression," MIT Press Books, 1.

The Economist, 2015a, "The Trust Machine," October 31 Issue.

_____, 2015b, "The Great Chain of Being Sure About Things," October 31 Issue.

Tirole, J., 2008, "Liquidity Shortages: Theoretical Underpinnings," *Banque de France Financial Stability Review: Special Issue on Liquidity*: 11, pp. 53–63.

United Nations Office of Drugs and Crime (UNODC), 2014,"Basic Manual on the Detection and Investigation of the Laundering of Crime Proceeds Using Virtual Currencies," June.

Vasek, M. and T. Moore, 2015, "There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams," *In Financial Cryptography and Data Security*, January 2015.

Weiss, L., 1980, "The Effects of Money Supply on Economic Welfare in the Steady State," *Econometrica: Journal of the Econometric Society*: 565–576.

White L.H., 1984, "Competitive Payments Systems and the Unit of Account," *The American Economic Review*, Vol. 74, No. 4, pp. 699–712.

Yellen, J., 2015, Normalizing Monetary Policy: Prospects and Perspectives, Speech at "The New Normal Monetary Policy," Research Conference.

Yermack, D., 2013, Is Bitcoin a Real Currency? An Economic Appraisal," (No. w19747). National Bureau of Economic Research.

Annex. Policy Responses to Virtual Currencies—Selected Countries

Jurisdictions have taken different approaches towards mitigating the potential risks of VCs and regulating VC-related activities. Following the Regulatory and Policy Challenges section, this Annex considers responses by selected jurisdictions that illustrate this divergence in approaches. [59]

Jurisdictions	AML/CFT: warning and regulating (existing and new)	Tax Treatment	Consumer Warnings and Advisories	Licensing/ Registration of VC Intermediaries	Financial Sector Warnings, and Bans	Bans on the Issuance/Use
Argentina	Warning on the ML/TF risks		Consumer Warning		Warning on reporting entities	
Bolivia						Yes
Canada	Amending existing regulations	Clarified tax treatment	Consumer Advisory			
China					Ban	
France	Application of existing regulations	Clarified tax treatment	Consumer Warning			
Germany	Application of existing regulations					
Italy			Consumer Warning		Warning	
Japan	Plan to introduce new regulations		Consumer Warning	Plan to introduce new regulations		
Russia	Application of existing regulations		Consumer Warning			Yes–draft law
Singapore	Plan to introduce new regulations	Clarified tax treatment	Consumer warning			
South Africa			Consumer Warning			
U.K.	Application of existing regulations	Clarified tax treatment				
U.S.	Application of existing regulations (Federal)	Clarified tax treatment (Federal)	Consumer Warning	State licensing regimes (for example, NY BitLicense)		

---

[59] The information gathered in the Annex includes readily available information from public sources and does not necessarily reflect all actions taken by any given jurisdiction.