



South African Reserve Bank

National Payment System Department

Position Paper on Virtual Currencies

Position Paper number 02/2014

Date issued: 2014-12-03

Version: Final

File Ref. no: 18/5/2-2014

1. Executive summary

1.1 This document outlines the position of the South African Reserve Bank (the Bank) on virtual currencies as it relates to the Bank's mandate and responsibilities. The document consists of five sections, i.e. the first three sections provide background, clarify concepts pertinent to the virtual currency discussion and draw a distinction between various categories of virtual currencies. The document further highlights several immediate risks associated with the current virtual currency landscape, in particular the decentralised convertible virtual currencies, and concludes with the Bank's position and responsibility in this regard as well as a caution to users of virtual currencies.

2. Background

2.1 A virtual currency (VC) is a digital representation of value that can be digitally traded and functions as a medium of exchange, a unit of account and/or a store of value, but does not have legal tender status¹. VCs constitute a leap away from the traditional banking and payment systems. The Financial Action Task Force (FATF) classifies VCs as either centralised or decentralised, and convertible or non-convertible². Convertible VCs have an equivalent value in real currency and can be exchanged back-and-forth for a real currency. Convertible VCs may be either centralised or decentralised VCs or crypto-currencies³ that are distributed, open-source, math-based peer-to-peer virtual currencies with or without a central administration, monitoring and oversight authority. Examples of decentralised VCs include Bitcoin (convertible), Litecoin and Ripple. In contrast, non-convertible VCs are centralised to a particular virtual community and cannot be exchanged for real currency. Examples of centralised non-convertible VCs include Q Coins and World of Warcraft Gold.⁴

¹ Financial Action Task Force : FATF Report "Virtual currencies key definitions and potential AML/CFT risks", June 2014, p 4

² Ibid p4

³ Crypto-currency refers to a math-based, decentralised convertible virtual currency that is protected by cryptography. Ibid p5

⁴ Ibid p4

- 2.2 Centralised non-convertible VCs tend to pose fewer risks to the general public given their closed nature to a particular community. Decentralised convertible VCs (DCVCs), on the other hand, are on the radar of many financial regulators worldwide due to their design and interaction with the real economy and currency. DCVCs were designed to create a type of “currency” which is entirely controlled by its users, removes ‘costly’ middlemen (commercial banks) from the transacting process and have the entire system open and available to the general public (block chains⁵).
- 2.3 DCVCs remove central banks/ monetary authorities, commercial banks and licensed money remitters from the payment process. The roles played by these entities are now performed and controlled by users of the DCVCs, as a collective i.e. money creation (a central bank function), safekeeping of deposits, transacting ability (a commercial bank business activity) and cross-border funds movements (irrespective of possible exchange controls). DCVCs tend to be traded between users with a high degree of anonymity. The emerging VC regulatory proposals are directed at managing the risks associated with DCVCs, hence the main focus of this paper on DCVCs.
- 2.4 Bitcoin is the leading type of DCVC in terms of value and volume, although relatively small compared to the larger financial ecosystem. The global market capitalisation of Bitcoin was said to amount to \$6, 25 billion, with the daily number of transactions averaging 60,000.⁶ Although DCVCs were originally mooted as independent ‘currency’, they are instead being treated as high-risk speculative investments by end-users due to their price volatility. Consequently, there is a substantial amount of hoarding and little real trade with DCVCs. Efforts from proponents attempt to change this dynamic by increasing merchant acceptance, integrating existing conventional payment instruments with DCVCs and promoting the advantages inherent in such systems. Thus, there is potential for real growth of Bitcoin in its current

⁵ A block chain refers to a public, electronic general ledger that records every payment and transfer of DC from the time of creation

⁶ Coeure, B, May 2014. Bitcoin and other decentralised virtual currency schemes: implications for central banks. Bank of International Settlements.

operational environment. In the Republic of South Africa (RSA), Bitcoins are traded through various platforms such as BitX which is an order matching system of buyers and sellers of Bitcoins.

3. Clarification of terms

3.1. Decentralised Convertible Virtual Currencies (DCVCs)

3.1.1 For the purpose of this document, the term DCVCs refers specifically to decentralised, crypto-currencies that interact with the real economy⁷ i.e. exchangeable for legal tender and may be used to purchase real world goods and services. As stated above, DCVCs are viewed as a subset of VCs.

3.2. Legal tender

3.2.1 In terms of the South African Reserve Bank Act, 1989 (Act No.90 of 1989) (“SARB Act”), the Bank governs the management of currency in RSA.

3.2.2 In terms of section 14 of the SARB Act, the SARB has the sole right to issue or cause to be issued banknotes and coins in RSA.

3.2.3 The SARB Act provides that a legal tender of payment of money is (section 17):

- a) a tender by the Bank itself, of a note of the Bank or of an outstanding note of another bank for which the Bank has assumed liability in terms of section 15 (3) (c) of the Currency and Banking Act or in terms of any agreement entered into with another bank before or after commencement of this Act; and
- b) a tender by the Bank itself, of an undefaced and un mutilated coin which is lawfully in circulation in RSA and of current mass.

3.2.4 Only the Bank is allowed to issue legal tender i.e. bank notes and coins in RSA which can be legally offered in payment of an obligation and that a creditor is obliged to accept. Therefore, DCVCs are not legal tender in RSA

⁷ FATF *op cit* p5

and should not be used as payment for the discharge of any obligation in a manner that suggests they are perfect substitute of legal tender.

3.3 Electronic-Money (E-Money)

3.3.1 E-money, as defined in the National Payment System Department Paper on Electronic Money 01/2009 (Electronic Money Position Paper),⁸ is electronically stored monetary value issued on receipt of funds and represented by a claim on the issuer. E-money is generally accepted as a means of payment by persons other than the issuer and is redeemable for physical cash or a deposit into a bank account on demand.

3.3.2 The Electronic Money Position Paper further declares that the issuance of E-Money as the business of a bank as defined in the Banks Act 1990 (Act No.94 of 1990). Therefore, there is a clear distinction between DCVCs and E-Money as DCVCs are tradable for cash while E-Money is redeemable for physical cash or a deposit into a bank account on demand.

4. Risks

4.1 The theoretical neutrality of any new payment instrument does not prevent it from being exploited for ambiguous or illegal purposes⁹. New payment mechanisms and innovations can facilitate greater flexibility, efficiency, speed and operational immediacy. DCVCs, in particular, may reduce the costs associated with the conventional banking system as these are perceived to be expensive. However, such innovations simultaneously provide a platform for, *inter alia*, money laundering and the financing of terrorism, and introduce a new set of risks to consumers as DCVCs are susceptible to misuse and at the very worst, have the ability to disrupt the financial system.

⁸ Available: [http://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem\(NPS\)/NPSLegislation/PositionPapers](http://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/NPSLegislation/PositionPapers)

⁹ Melonghi G "Fighting financial crime in the age of electronic money: opportunities' and limitations" 2001 *Journal of Money Laundering Control* 206 – 207

4.2 Additionally, there are many legal uncertainties regarding virtual currency schemes (including DCVCs). The lack of a proper regulatory and legal framework substantially exacerbates the other risks, especially the enforcement of the principle of finality and irrevocability in the payment systems.¹⁰ Furthermore, no specific regulatory protection exist that would compensate the owner or user of DCVCs for any loss that may be suffered, should the DCVC fail or the business ceases to exist. In this regard, users need to be warned that they might lose their money.

4.3 The following risk elements are considered particularly significant:

4.3.1 *Payment systems and payment service providers*

4.3.1.1 Payment system oversight is aimed at ensuring the payment system's safety and efficiency. Failure of payment services providers (PSP) that provide services in real currency and VCs to meet contractual obligations in the VC environment could potentially pose risks to the safety of the payment systems. The possible sources of failure vary from liquidity exposures, the anonymity of some counterparties, failure to hold sufficient VC units to settle transactions, VCs' price volatility and lack of transparent price formation. This could further be exacerbated by inadequate liquidity management of the PSP which may intensify the need for liquidity and operational problems in linking real currency and VC (e.g. settlement failure, outages, capacity, fraud and data loss).¹¹ Reputational risks and losses could also arise where VCs are offered to existing customers, leading to the association of unregulated VCs with regulated products.

4.3.1.2 DCVCs are also susceptible to credit and liquidity risks, which could have a destabilising effect on the stability of the payment system. Given the absence of guaranteed settlement of current or future financial obligations, end-users are exposed to credit risk in relation to any funds

¹⁰ European Central Bank: Virtual Currency Schemes, October 2012 Frankfurt am Main: European Central Bank, p.40

¹¹ European Banking Authority: "EBA Opinion on Virtual Currencies" , July 2014, p35

held on the virtual accounts. Liquidity risk is equally possible where a settlement institution fails to meet any commitments it has made to provide liquidity to the participants as and when expected. Due to the illiquid nature of DCVCs, the conversion of users' funds into real money would probably not occur quickly enough and without a significant material loss in value.¹²

4.3.2 Price stability

4.3.2.1 The European Central Bank (ECB),¹³ argued that price stability could be affected where VCs (in general) substantially modify the quantity of money, have an impact on the velocity of money, the use of cash, and/or influence the measurement of monetary aggregates, and where there is an interaction between the VC and the real economy. VCs could have an impact on price stability and monetary policy if they affect the demand for the central bank's liabilities and interfere in the control of money through open market operations.

4.3.2.2 According to the ECB, wide acceptance of VCs could have a substitution effect on central bank money, thereby reducing the need for cash needed to conduct the transactions generated by nominal income, reducing the central bank balance sheets and their ability to influence the short-term interest rates. The ECB concluded that although the continued stable issuance of money indicates that DCVCs do not pose significant risks at this stage, continued monitoring of the interaction between VCs and the real world was highly necessary.

4.3.3 Anti-money laundering and combating the financing of terrorism

4.3.3.1 The risk-based approach applied to anti-money laundering (AML) and countering of financing of terrorism framework (CFT) , led by, *inter alia*,

¹² Ibid, p40

¹³ European Central Bank, *Op cit*, p34

the Financial Action Task Force (FATF) and the European Union (EU), highlighted the importance of identifying money laundering and financing of terrorism risks associated with emerging payment mechanisms and/or products such as VCs.

4.3.3.2 The traditional phases of placement, layering and integration can easily be combined at an information technology (IT) level through electronic channels. At the placement phase specific relevance is given to instruments that allow the sender to transfer funds directly to the recipient, resulting in the bypass of traditional AML/CFT systems, which are based on identification and monitoring of transaction movements. Due to the high degree of anonymity, the use of DCVCs in transactions bypasses these traditional anti-money laundering systems. Criminals are therefore able to launder proceeds of crime due to the ease of anonymous, rapid and irrevocable deposits and transfers¹⁴.

4.3.3.3 With no central repository, law enforcement, payment processors and financial institutions have little control over DCVCs. Furthermore, as a result of the de-materialisation of monetary exchange and payment service, combined with a loss of direct contact with the client, such technologically advanced instruments have a low degree of transparency. AML and CFT regulations rely on financial institutions as an additional layer of protection in the process of guarding payment systems. Through peer-to-peer movements, value or payment can be facilitated without reliance on financial institutions or professionals acting as an intermediary.

4.3.3.4 Furthermore, the anonymity provided through the use of DCVCs, in transferring value makes it very attractive for financial abuse across different jurisdictions. The FATF has in numerous reports highlighted the potential of financial abuse of any financial product which has the capability to mask ownership and identity, whether intentionally through

¹⁴ European Banking Authority: "EBA Opinion on Virtual Currencies" , July 2014, p14

product design or operational use. Both the FATF and the EU Directive on money laundering¹⁵ echo the recognition of greater risks of non-face-to-face transactions and recommend the application of enhanced due diligence.

4.3.3.5 The lack of transactional record keeping becomes a problem when trying to reconstruct illicitly performed transactions. In the case of DCVCs, transferred information is published in the software itself and attempting to trace the Internet Protocol (IP) address becomes questionable. The identification of relevant laws applicable to the contravention and the consequent gathering of evidence regarding a transaction can become an unattainable task. Compared to conventional currencies, DCVCs are less susceptible to freezing or seizure actions by law enforcement agencies.

4.3.3.6 A final money laundering risk consideration, relates to the speed and ease with which DCVCs transactions can be carried out. By avoiding the limitations of physical currency, it allows for the rapid transmission of a substantial sum of value i.e. single transactions or cumulative process of multiple transactions.

4.3.4 Consumer Risk

4.3.4.1 The unregulated nature of VCs (generally) exposes end-users to risks. One of the greatest risks for end-users trading in DCVCs is the potential to incur sizeable financial losses. This is often a result of the price volatility inherent in DCVCs as demand and supply (price) are controlled by individuals and could fluctuate wildly.

4.3.4.2 Other potential risks to consumers¹⁶ include the following:

¹⁵ Directive 2005/60/EC of the European Parliament and the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, 2005

¹⁶ The Clearing House : “ Virtual Currency: Risks and Regulation” , June 2014 p4

- a) Loss or theft through a security breach, user error, or a technological failure at a VC wallet or exchange. Once lost, virtual currency typically cannot be regained.
- b) Fraud or unauthorized use by anyone in possession of the associated ownership credentials. Transactions in most currencies are not reversible, even if the result of fraud or unauthorised use.
- c) Transaction processing error in the event that a payment is misdirected, an incorrect amount is transferred, or a transaction is not completed in a timely manner due to an error by a VC wallet, exchange, or processor, in most currencies the transaction is not reversible, the error is not correctible, and the consumer has no recourse against the wallet, exchange, or processor.
- d) Absence of insurance mechanism to make accountholders whole in the event that a VC wallet or exchange operator fails and accounts become inaccessible.
- e) Wallets and exchange operators have no obligation to provide disclosures to consumers related to service fees or charges associated with VC transactions, the volatility and unregulated nature of the virtual currency ecosystem, or any of the other risks described in this table.

4.3.5 Circumvention of Exchange Control Regulations

4.3.5.1 The main objective of Exchange Control Regulations, 1961 (Regulations)¹⁷ is to prevent the loss of foreign currency resources through the transfer abroad of real or financial capital assets held in RSA,

¹⁷<http://www.resbank.co.za/RegulationAndSupervision/FinancialSurveillanceAndExchangeControl/Legislation/Documents/ExchangeControlRegulations1961.pdf>

as well as constitute an effective system of control over the movement into and out of RSA of financial and real assets.

4.3.5.2 In terms of the Regulations, South African residents are afforded a foreign capital allowance of R4 million per calendar year. These funds may be transferred abroad and invested in any manner without prior approval from the Financial Surveillance Department of the Bank (FinSurv), provided a tax clearance certificate is obtained. The anonymity of transactions in respect of DCVCs have the potential to result in exchange control circumvention as the transfer would not be effected and reported by an Authorised Dealer in foreign exchange. Should investors choose to acquire DCs in terms of their foreign capital allowance, they do so at their own risk and have no recourse to South African authorities.

4.3.5.3 The transfer of DCs in and out of RSA are not supported by the Regulations, therefore, requests to trade in DCs cross-border cannot be authorised by the Bank and if any such trades do take place, the risks associated with such trades are for the participants in such trades. FinSurv would not be in a position to report on the “flow” of DCVCs because the transactions would not be reported on the FinSurv Reporting System. It follows that payments using DCVCs in respect of imports or the receipt of export proceeds would not be detected and as a consequence FinSurv would not be able to report thereon.

4.3.5.4 VCs in general can exert significant competitive pressure on existing payment systems, especially for low value and long distance cross border transactions such as remittances, which are deemed to be rather costly. If network effects take hold, they could divert an increasing stream of payments away from established retail payment infrastructures.

4.3.6 *Financial stability*

- 4.3.6.1 The main sources of financial instability in the context of DCVCs would be the link between DCVCs and the real economy and where DCVCs jeopardises the smooth functioning of payment systems.¹⁸
- 4.3.6.2 The Bank is continually monitoring and analysing market and other financial and economic factors, to identify and mitigate systemic risks by implementing appropriate policies, and assessing the potential impact of these policies on the broader financial system.
- 4.3.6.3 Values (\$6,25 billion) and volumes (60 000 daily average) currently traded in Bitcoin (the leading DCVC) remain insignificant when compared to the formal payment system and the larger economy. VCs are not considered legal tender in most jurisdictions. A multitude of independent variants of VCs exist and are being developed, all aimed at the same niche market. Based on the aforementioned, VCs (particularly DCs), at this stage of their development, are neither broad nor evasive enough to be classified as systemic. However, constant monitoring of DCVCs is necessary.

5 Conclusion

- 5.1 The Bank does not oversee, supervise or regulate the VC landscape, systems or intermediaries for effectiveness, soundness, integrity or robustness. Consequently, any and all activities related to the acquisition, trading or use of VCs (particularly DCVCs) are performed at the end-user's sole and independent risk and have no recourse to the Bank.
- 5.2 Given the current landscape and information currently available, the Bank contends that VCs pose no significant risk to financial stability, price stability or the National Payment System. However, end-users, whether individuals or businesses that accept VCs and businesses involved in the VCs ecosystem,

¹⁸ European Central Bank: *op cit* p37 & 38

are cautioned that any activities performed or undertaken with VCs are at their sole and independent risk.

- 5.3 In line with the Bank's position that regulation should follow innovation, the Bank continues monitoring developments in this regard and reserves the right to change its position should the landscape warrant regulatory intervention.