JOURNAL OF ANTI-CORRUPTION LAW

2018 Volume 2 Number 2 Pages 163 - 182

Bitcoin Regulation? Imperfect Knowledge of Identities and the Money Laundering Risk: A West African Perspective*

Egbiri Ifegwu Egbiri**

Nkechikwu Valerie Azinge***

ABSTRACT

Arguments for regulating Bitcoin are built mainly on the technologically disruptive nature of the currency and its susceptibility to facilitating financial crimes on a scale larger than financial institutions. This paper questions this notion and proposes instead that the disruptive nature of Bitcoin is not technological but legal. The legal disruption requires a legislative response aimed at ensuring suitable regulation that can circumvent the identity crises in Bitcoin transactions.

1 INTRODUCTION

Technological innovations for financial exchanges evolve at a rather fast pace. Most times, the evolution happens in ways that regulators cannot foresee or with which they cannot keep pace. The evolution of cryptocurrencies is a striking recent example in this regard. Given the volume of anonymised transactions effected through this medium, experts view cryptocurrencies with scepticism, arguing that

---

* This is a revised version of a paper read at the *Economic Crime and Cybercrime Conference (ECCC)*, University of the Western Cape, 5 October 2018.

** LLB (University of Nigeria), LLM (New York University). Principal Legal Counsel, African Development Bank (AfDB). Email: e.egbiri@afdb.org.

*** LLB (University of Leicester), LLM, PhD (University of Warwick). Lecturer, University of Lincoln. Email: nkazinge@gmail.com.

they serve as a site of economic crimes, such as money laundering.[1] It is argued that cryptocurrencies, like Bitcoin, add extra layers of anonymity by allowing users to transfer value without the tailored customer due diligence (CDD) that is applicable to users of most conventional financial institutions.[2] The Bitcoin community resents such representation, arguing that its public accounting process allows for transparency on every transaction and therefore is not necessarily a money laundering facilitator.

It must be noted, however, that transaction identity is not ownership identity.[3] The Bitcoin accounting process relies on aliases and encrypted codes which unveil the transaction history of users but seemingly is unconnected with the identity of the owner. User anonymity is facilitated also by software such as BitLaundry,[4] thereby amplifying arguments that launderers can exploit the perfect knowledge of transactions owing to the masks provided by the imperfect knowledge of identities. This furthers the discourse that Bitcoins are a disruptive alternative for laundering money. Efforts to promote anonymity are countered by gatekeepers, such as Coinbase, which require adequate CDD for trade in Bitcoins, a

1 Bryans D (2014) "Bitcoin and Money Laundering: Mining for an Effective Solution" 89 *Indiana Law Journal* 421-472 at 441; Kien-Meng Ly M (2014) ''Coining Bitcoins 'Legal-Bits': Examining the Regulatory Framework for Bitcoin and Virtual Currencies" 27(2) *Harvard Journal of Law & Technology* 588-608 at 595; Van Wegberg R (2018) "Bitcoin Money Laundering: Mixed Results? An Explorative Study on Money Laundering of Cybercrime Proceeds Using Bitcoin" 25(2) *Journal of Financial Crime* 419–435 at 420.

2 CDD is the process of identifying and verifying a financial/non-financial institution's customer. In practice, this entails obtaining the customer's names, photograph and official documents which confirms identify, address, date of birth and the like. See FATF (November 2017) "FATF Guidance on AML/CFT Measures and Financial Inclusion with a Supplement on Customer Due Diligence", available at http://www.fatf-gafi.org/media/fatf/content/images/Updated-2017-FATF-2013-Guidance.pdf (visited 10 January 2019).

3 The identity of a Bitcoin usually remains unknown in the process of transactions. However, every transaction on the network is documented in the ledger. This is explained further in §2 below. The problem is that traditional CDD requirements are focused on the identity of customers as a means of curtailing money laundering. In the absence of the identity, institutions and their regulators struggle to trace laundering with only the map of transactions. Note however, that even transaction identity sometimes can be spoofed. See Turpin J (2014) "Bitcoin: The Economic Case for a Global, Virtual Currency Operating in an Unexplored Legal Framework" 21(1) *Indiana Journal of Global Legal Studies* 335-368 at 339.

4 BitLaundry allows for the distortion of transaction logs, so that customers deliberately receive different Bitcoins from the ones originally transferred. See Matonis J (5 June 2013) "The Politics of Bitcoin Mixing Services" *Forbes*, available at https://www.forbes.com/sites/jonmatonis/2013/06/05/the-politics-of-bitcoin-mixing-services/#70d9ea45302e (visited 10 March 2019).

process which can lead to uncovered identity.[5] Therefore, the extent to which Bitcoins are disruptive of existing money laundering processes is questionable.

Nevertheless, the problems posed by the imperfect knowledge of identities present a grey area for law, particularly in West African countries. Current regulatory approaches are inadequate in that they focus on combating money laundering through the conventional "lens of the perfect knowledge of identities", an approach which would be futile in combating the use of Bitcoin for money laundering purposes. Hence, this paper advances the need for a principle-based legal approach which encourages technological innovation, whilst adequately addressing money laundering concerns in the cryptocurrencies medium.

The core argument of this paper is that the current disruptive nature of Bitcoin as regards the facilitation of money laundering is of a legal kind and not yet of a technological nature. Hence, there has to be a fundamental change in the law aimed at accommodating technological advances and ensuring its continued relevance in relation to innovative laundering processes. Against this background, the paper starts by demystifying the concept of Bitcoin and investigating the processes that comprise the Bitcoin network. Thereafter, the focus will turn to appraising the presumed technologically disruptive nature of Bitcoin *vis-à-vis* money laundering. This is amplified by an examination of the variations in laundering processes through financial institutions and underground banking. The paper then considers the legal disruption of Bitcoin by analysing the limits of the current approach taken by some West African countries. The West African region is under scrutiny because of the intermittent and varying steps taken by its constituent countries to control the money laundering risks associated with Bitcoin.

2 UNDERSTANDING THE BITCOIN ECOSYSTEM

Put simply, a Bitcoin is a chain of signatures (a string of numbers) saved in a "wallet file".[6] These signatures encompass the history of each specific Bitcoin to allow the system authenticate its legitimacy and transfer ownership from one user to another upon request.[7] Each user's wallet contains their Bitcoins, a public key and

5 Coinbase is a digital currency wallet and platform where merchants and customers can transact with digital currencies such as Bitcoin. See Coinbase (2019) "Buy and Sell Cryptocurrency", available at https://www.coinbase.com/about (visited 18 January 2019); As the third largest virtual wallet, Coinbase requires rigorous identity verification. See Scott S "Cryptocurrency Compliance: An AML Perspective" (ACAMS: Advancing Financial Crime Professionals Worldwide), available at http://files.acams.org/pdfs/2017/Cryptocurrency_Compliance_An_AML_Perspective_S.Scott.pdf (visited 10 January 2019).

6 Turpin (2014) at 337.

7 Turpin (2014) at 337.

a private key.[8] Whilst the public key is the address to which a person can send Bitcoins, the private key is what permits the wallet's owner to send his Bitcoins to a different party.[9] Turpin likens the public key to your street address and the private key to your house key. He states that "whilst others can send mail to your house with no more than your address … no one can remove your belongings without your permission".[10]

Bitcoins, like the constituent elements of most cryptocurrencies, are generated by and operate solely on digital algorithms. Miners decode the algorithms using software backed by computers with great processing powers to generate additional units of the currency, with which they then can trade or transact.[11] Users of this currency do business in Bitcoin exchanges through peer-to-peer transactions.[12] These exchanges go through the bitcoin wallet of users and are processed by a large network of computers running specialised software simultaneously.[13] Whenever such transactions occur, the network reports the payer's and recipient's addresses, which are number-based codes.[14] Both parties to the transaction remain anonymous, except for the equivalent of an account number — the signature. The transactions then are entered into a ledger/record called a blockchain. The blockchain is updated every day and sent to each computer which processes Bitcoins, to facilitate verification against counterfeiting.

Bitcoin merchants operate in countries where the currency is accepted for payment of goods and services. Although described largely as a medium of exchange which acts like a currency in some environments, cryptocurrencies do not have the attributes of a real currency.[15] So, although cryptocurrencies are accepted as payment for goods and services or even used as a store of value, they are not recognised as a legal currency. Rather they are decentralised. This simply means that their value is not backed or administered by any centralised issuing

8 Turpin (2014) at 337.
9 Turpin (2014) at 337.
10 Turpin (2014) at 338.
11 PwC (2014) "Cryptocurrency – The Next Wave of Disruption or Storm in a Teacup?", available at http://www.digitalinnovation.pwc.com.au/cryptocurrency-next-wave-disruption/ (visited 10 March 2019).
12 Kien-Meng Ly (2014) at 592.
13 Chang J (30 October 2013) "First Bitcoin ATM Installed in Vancouver Coffee Shop" *ABC News*, available at https://abcnews.go.com/Technology/bitcoin-atm-conducts-10000-worth-transactions-day/story?id=20730762 (visited 10 March 2019).
14 Bryans (2014) at 443 & 446.
15 Kien-Meng Ly (2014) at 589.

institution controlling the intake of consumers or setting monetary value.[16] In essence, cryptocurrencies lack legal tender status in most jurisdictions and their value is set by user demand and supply.[17]

Notwithstanding the uniqueness of Bitcoin, it does display certain characteristics that are crucial for fiat currency.[18] For instance, Bitcoin has been limited to 21 million coins, as a way of ensuring scarcity whilst keeping inflation low.[19] What is more, in the face of the dangers associated with online exchanges, Bitcoin has strived to ensure a measure of security for its members, particularly through its blockchain recording framework.[20] Further, Bitcoin aims to simplify its transfer processes which can be done through a mobile device.[21] Transfers usually are instantaneous and eliminate the need for a "trusted intermediary", thereby reducing or possibly eliminating transaction costs. Also, Bitcoin allows for a large volume of unregulated transactions.[22] Given the apparent competitive advantage of Bitcoin relative to other means of transfers, PwC concludes that:

> cryptocurrencies are clearly gaining traction for both consumers and businesses, and this is likely to continue as consumers desire private, secure forms of currency.[23]

It is crucial, however, to decipher whether Bitcoin is particularly attractive for laundering purposes, especially in West African countries.

3 BITCOIN: DISRUPTING ESTABLISHED MONEY LAUNDERING PROCESSES IN WEST AFRICA?

The introduction of Bitcoin signified huge technological advancement in the financial industry in West African countries, as it provided a cost effective method of effecting micropayments in the region. Such advancement hinged on the

16 Mantonis J (3 November 2012) "ECB: 'Roots of Bitcoin Can Be Found in the Australian School of Economics'" *Forbes*, available at https://www.forbes.com/sites/jonmatonis/2012/11/03/ecb-roots-of-bitcoin-can-be-found-in-the-austrian-school-of-economics/#30df727c3b18 (visited 20 March 2019).

17 Bryans (2014) at 443-445.

18 Baur A, Buhler J, Bick M & Bonorden C (October 2015) "Cryptocurrencies as a Disruption? Empirical Findings on User Adoption and Future Potential of Bitcoin and Co" *Open and Big Data Management and Innovation Conference*, The Netherlands.

19 Papp J (2014) "A Medium of Exchange for an Internet Age: How to Regulate Bitcoin for the Growth of E-Commerce" 15 *Journal of Technology, Law & Policy* 33-56 at 43.

20 Bayern S (2014) "Dynamic Common Law and Technological Change: The Classification of Bitcoin" 71(2) *Washington and Lee Law Review Online* 1-34 at 22

21 Baur *et al* (October 2015).

22 As at January 2019, one Bitcoin was equated to 3 635 USD, meaning that the transfer of 10 Bitcoins, which will equate to 36 350 USD, would not be regulated.

23 PwC (2014).

exponential growth in the use of smart mobile technology in Africa.[24] Studies indicate a 35.2% mobile internet penetration in Africa in 2017, signalling a 9% growth from 2000-2017.[25] Additionally, mobile penetration is currently at 80% in Africa, with a marked projection for increase by 2020.[26] The growing base of internet and mobile technology in West African countries has created an atmosphere conducive for cryptocurrencies and blockchain initiatives to thrive. For instance, mobile money platforms such as M-Pesa, which created an avenue for cryptocurrencies to thrive in Kenya,[27] now enjoys widespread use in West Africa.[28] This achievement suggest that Bitcoin indeed may serve as a tool for increased financial inclusion, thereby encroaching into an area — the transfer of funds — that used to be reserved for financial institutions and the informal sector[29] and in which money laundering and its predicate offences already were entrenched.

The anonymity of identity provided by Bitcoin, coupled with the volume of transfer it permits, has heightened the fear that launderers would be most likely to use this medium of transfer. Chiu submits that cryptocurrencies are prone to being used for illicit purposes.[30] She points to the Silk Road Online Marketplace case,

24 Mapp M & Mwaita P (6 July 2017) "Report of the Second Roundtable Discussion on Cryptocurrency and Blockchain Regulation in Uganda" (United Nations African Institute for the Prevention of Crime and the Treatment of Offenders and the University of Birmingham) at 8.

25 Internet World Stats "Internet Penetration in Africa: December 31, 2017", available at https://www.internetworldstats.com/stats1.htm (visited 20 March 2019).

26 All Africa (25 April 2017) "Africa: Mobile Penetration in Africa Hits 80pc", available at https://allafrica.com/stories/201704251054.html (visited 20 March 2019); Global Systems for Mobile Communications Association (GSMA) "The Mobile Economy 2018", available at https://www.gsma.com/mobileeconomy/wp-content/uploads/2018/05/The-Mobile-Economy-2018.pdf (visited 20 March 2019).

27 BitcoinPrBuzz (3 April 2017) "BitHub.Africa Announces African Blockchain Opportunity Crowd Sale Campaign to Foster Region's Cryptocurrency Ecosystem", available at https://bitcoinprbuzz.com/press-release-bithub-africa/ (visited 21 March 2019).

28 Although mobile money originated in East Africa, West Africa has emerged as the new mobile money frontier. See Gahigi M (27 July 2017) "Mobile Money Is Only Just Starting to Transform Some of Africa's Markets" *QuartzAfrica*, available at https://qz.com/africa/1039896/m-pesa-mtn-orange-others-lead-africas-mobile-money-revolution/ (visited 10 January 2019).

29 The informal sector, black market or underground market refers to the provision of services (legal or illegal) which escape detection in the official estimates of GDP. It is economic activity that is hidden from public authorities. See Tanzi V & Schuknecht L (1997) "Reconsidering the Fiscal Role of Government: The International Perspective" 87(2) *American Economic Review* 164-168 at 168.

30 Bank for International Settlement: Committee on Payment and Settlement Systems (2003) "A Glossary of Terms Used in Payments and Settlement Systems", available at https://www.bis.org/cpmi/glossary_030301.pdf (visited 21 March 2019).

where cryptocurrencies were used to purchase drugs under the cloak of anonymity.[31] Conceding the point, JPMorgan observes that:

> the only area where cryptocurrencies could compete with national currencies as a medium of exchange is in the black market.[32]

The dwindling institutional trust in financial regulators fuelled the drive towards the use of Bitcoin in West African countries for both legitimate and illegitimate transactions. For instance, in 2015 millions of Nigerians were defrauded of funds in excess of 11.9 billion naira[33] through Mavrodi Mundial Moneybox (MMM), which had a Bitcoin platform and was promoted as a pyramid network for circulating wealth.[34] Also, Niger and Nigeria were hit by the Wannacry ransomware, which demanded ransom payments in Bitcoins to avoid obliteration of core documents in computer files.[35]

The incidence of laundering via Bitcoins has occasioned arguments that they provide an avenue for expanded laundering and therefore is disruptive of the current payment systems, particularly the underground market. The financial payment systems are arguably most affected by Bitcoin laundering, as the latter circumvents the CDD processes, thereby earning this "currency" the tag of

31 Trautman L (2014) "Virtual Currencies Bitcoin and What Now: After Liberty Reserve, Silk Road, and MT Gox?" 30 *Richmond Journal of Law and Technology* 1-108 at 13.

32 RT (17 February, 2018) "No Chance of Cryptocurrencies Replacing Fiat Money — JPMorgan", available at https://www.rt.com/business/419081-jpmorgan-cryptocurrencies-hurdle-money/ (visited 20 March 2019).

33 Ujah E (31 May, 2017) "How Nigerians Invested over N28.7bn, Lost N11.9bn in Crashed MMM" *Vanguard*, available at https://allafrica.com/stories/201705310447.html (visited 21 March 2019).

34 Hegarty S (16 December 2016) "Nigeria's MMM Ponzi Scheme: Will Investors Get their Money?" *BBC News*, available at http://www.bbc.co.uk/news/world-africa-38340457 (visited 21 March 2019); Findlay S (7 February 2018) "Nigerian Cryptocurrency Craze Unfazed by Bitcoin Plunge" *Phys.org*, available at https://phys.org/news/2018-02-nigerian-cryptocurrency-craze-unfazed-bitcoin.html (visited 21 March 2019); Barabas C (13 October 2017) "Bitcoin's Rise in African Markets is Driven by an Old Russian Ponzi Scheme" *Quartz Africa*, available at https://qz.com/1100886/bitcoin-in-africa-is-driven-by-mmm-mavrodi-ponzi-scheme/ (visited 20 March 2019).

35 Akwei I (15 May 2017) "Africa Least Hit by WannaCry Ransomeware Cyber-Attack *AfricaNews*, available at http://www.africanews.com/2017/05/15/africa-least-hit-by-wannacry-ransomware-cyber-attack// (visited 21 March 2019); McDonnell T (22 January 2018) "How Nigerians Beat Bitcoin Scams" *Bloomberg Businessweek*, available at https://www.bloomberg.com/news/articles/2018-01-22/how-nigerians-beat-bitcoin-scams (visited 21 March 2019).

"disruptive innovation". However, "disruptive innovation" does not refer necessarily to technological advancements in a particular market,[36] but rather to:

> the process where an entrant takes root at the low-end of the market or in a new market and, through subsequent improvements, moves up-market, eventually displacing competitors.[37]

This begs the questions: Are launderers more inclined to using cryptocurrencies as a medium of payment or transfer? Does this displace existing transfer structures? A response to these questions warrants a critical examination of money laundering processes.

3.1 Traditional Money Laundering Processes

Money laundering is the process of making dirty money clean by it from its criminal origin. Where, for instance, profit is derived from any illicit activity, such as trafficking of narcotic drugs or corruption,[38] those involved must devise a means to control the funds without bringing notice to themselves or their criminal activity.[39] Criminals achieve this by concealing the source of the funds, altering their form or transferring them to less conspicuous environments.[40]

The process of money laundering has been distilled into three phases: placement, layering and integration.[41] Money generated from illicit activities is introduced into the financial system or underground market at the placement stage. At this level, the proceeds of crime are easily detectable by the authorities. In order to avoid being caught, launderers fragment the lump sum and employ a variety of techniques, such as cash deposits and the purchase of monetary instruments, property or luxury items, to distance the illicit funds from their source.[42] Once this is achieved, launderers further conceal the source and ownership of the funds by converting, moving or investing them, predominantly in offshore jurisdictions.[43] This complex web of transfers, which sometimes involves

36 Schmitz S (14 November 2006) "The Political Economy of Institutional Change in Payment Systems and Monetary Policy" *SSRN*, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=944404 (visited 20 March 2019).

37 Christensen CM, Raynor M & McDonald R (2015) "What Is Disruptive Innovation?" 93 *Harvard Business Review* 44-53 at 44.

38 FATF "Designated Categories of Offences", available at http://www.fatf-gafi.org/glossary/d-i/ (visited 21 March 2019).

39 Irwin A, Choo K-K & Liu L (2011) "An Analysis of Money Laundering and Terrorism Financing Typologies" 15(1) *Journal of Money Laundering Control* 85-111 at 95.

40 Irwin, Choo & Liu (2011) at 95.

41 Irwin, Choo & Liu (2011) at 86.

42 Irwin, Choo & Liu (2011) at 93.

43 FATF "Designated Categories of Offences".

the creation of sham businesses, is aimed at frustrating any attempts at identifying a paper trail. To finalise the laundering process, launderers usually reintroduce the funds into the legitimate economy. They utilise investment in real estate, luxury assets or business ventures to enable them retain their illicit profits whilst, at the same time, ensuring their freedom. However, these processes are not always sequential and may sometimes overlap.

Laundering usually occurs through financial or designated non-financial institutions in developed countries.[44] The CDD requirements in these institutions ideally allow for perfect knowledge of identities. Developing countries in West Africa have a varying trajectory, and although financial and non-financial institutions are present, launderers may take advantage of the cash-based economy.[45] This is a concern for regulators who fear that the cash-based economy has become the basis of most untraced crimes.[46] For instance, in Nigeria, $43 million in cash were found in a Lagos apartment believed to be funds corruptly derived from the government and owned by unnamed politicians. The discovery of hidden cash, which is common in Nigeria, is attributable partially to the whistle-blowing policy introduced to combat corruption.[47] For this reason, Bitcoin may indeed become a preferred money laundering option. The attraction is that Bitcoin allows for transfers and payments at instantaneous speed, without risk of interception, because of the privacy it offers.[48]

3.2 Bitcoin Laundering: Imperfect Knowledge of Identities and its Disruptiveness

A classic Bitcoin laundering event includes various stages. It should be observed, however, that these stages mirror those of the traditional laundering process. Firstly, funds derived from illicit activities are used to purchase Bitcoin directly; or

---

44 Patel H & Thakkar B "Money Laundering Among Globalized World", available at http://cdn.intechopen.com/pdfs/38372/InTechMoney_laundering_among_globalized_world.pdf (visited 10 January 2019).

45 Uche C "Money Laundering: A View from a Developing Country", available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.600.9343&rep=rep1&type=pdf (visited 10 January 2019).

46 Mynhardt R & Marx J "Anti-Money Laundering Recommendation for Cash-Based Economies in West Africa"., available at https://virtusinterpress.org/IMG/pdf/Ronald_H_Mynhardt_Johan_Marx_paper.pdf (visited 10 March 2019).

47 Kazeem Y (13 February 2017) "Nigeria's Whistle-Blower Plan to Pay Citizens to Report Corruption is off to a Great Start" *Quartz Africa*, available at https://qz.com/909014/nigerias-new-corruption-whistle-blowing-policy-is-helping-the-government-recover-looted-funds/ (visited 10 March 2019).

48 Bryans (2014) at 443-445.

they may be used to acquire gift cards or pre-paid visa cards which are then used to purchase Bitcoins. These funds are sometimes transferred from an overseas jurisdiction to a recipient in another country who purchases Bitcoins on behalf of the payer. Secondly, the Bitcoins then are tumbled to distance them from there source, either by using them as a means of payment or selling them in bits to other users. Thirdly, miners may be employed to spoof Bitcoin verification. In addition, Bitcoin identity can be hidden through the use of virtual private networks (VPNs) to conceal the Internet Protocol (IP) address. Lastly, currency exchangers can facilitate the conversion of Bitcoins to other currencies and vice versa.[49] The marked similarities between Bitcoin laundering and fiat laundering have occasioned arguments that Bitcoin did not change the process of laundering.[50] Remarkably, however, at all stages of the Bitcoin laundering process, the anonymity of the Bitcoin owner is preserved but the transaction history usually is made public through the ledger. For this reason, technological experts have argued that the Bitcoin public accounting process allows for transparency on every transaction, thereby forestalling laundering.[51]

Transaction identity is, however, not ownership identity. The Bitcoin accounting process relies on aliases and encrypted codes, which are not associated with the true identity of the owner. Without being able to tie an identifiable user to a single Bitcoin address, it would be difficult for enforcement officers to track the injection, layering or re-entry of laundered funds.[52] The notorious Silk Road Online Marketplace case involved exploitation of this loophole, with Bitcoin being used to facilitate payment for illegal drugs and weapons. All the relevant parties were cloaked in anonymity and enforcement officers struggled to bring the scheme to an end.[53] Likewise, in Nigeria, MMM and other ponzi schemes, operated through their Bitcoin platforms, have disappeared into thin air, along with investors' funds.[54] This laundering occurred despite efforts of gatekeepers — such as Coinbase — which require adequate CDD to trade in Bitcoins. Moreover, these

49 Kien-Meng Ly (2014) at 589.

50 Bohannon J (9 March 2016) "Why Criminals Can't Hide Behind Bitcoin" *Sciencemang.org*, available at http://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin (visited 21 March 2019).

51 Bohannon (9 March 2016).

52 Buterin V (27 November 2012 "Block Reward Halving: A Guide" *Bitcoin Magazine*, available at https://bitcoinmagazine.com/articles/block-reward-halving-a-guide-1354053560/ (visited 21 March 2019).

53 Ball J, Arthur C & Gabbatt A (2 October 2013) "FBI Claims Largest Bitcoin Seizure after Arrest of Alleged Silk Road Founder" *The Guardian*, available at https://www.theguardian.com/technology/2013/oct/02/alleged-silk-road-website-founder-arrested-bitcoin (visited 21 March 2019).

54 Ujah (31 May 2017).

efforts are countered by such applications as BitLaundry which are focused on providing increased anonymity to Bitcoin users. Thus, launderers can exploit the perfect knowledge of transactions using the mask provided by the imperfect knowledge of identities. For this reason, experts have viewed cryptocurrencies with scepticism, arguing that they serve as a platform for crimes such as money laundering.[55]

Having established that Bitcoins can be used to facilitate money laundering, it is necessary to discuss whether it is disruptive to existing laundering processes. Simply put, does Bitcoin have a competitive advantage over other forms of laundering, particularly the underground market which is predominant in West African countries? Would launderers prefer to use Bitcoin over the alternatives? There is no straightforward answer as a launderer's options vary. A rational launderer may consider factors such as profit maximisation, leverage potential, exposure of transaction record, acceptability, security, and transfer time.[56] However, most payment systems have these characteristics.[57] Hence, it is imperative to ask: Why Bitcoin?

Anonymity of identity is flaunted as the feature which distinguishes Bitcoin from other payment systems. The anonymity feature makes Bitcoin more attractive for laundering, given that it is believed to derail attempts by the authorities to identify launderers. Dostov & Shust disagree and argue that authorities may exploit certain loopholes, such as the delivery and usage of purchased items or currency, which provide clues about the laundering patterns.[58] Furthermore, the linkage between payment transactions aids in investigations. These were evident in the Silk Road Online Marketplace case. Also, in cases of theft or loss, launderers may be unable to assert proprietary rights.[59] In this regard, Chiu stresses that physical cash can be protected from loss of theft through criminal, tort and property law.[60] Additionally, for depositors and, indeed, payment transfers, the state guarantees a form of deposit protection;[61] and for investments, protection in the form of proprietary rights exist even when the

55 Bryans (2014) at 441; Kien-Meng Ly (2014) at 589.
56 Dostov V & Shust P (2014) "Cryptocurrencies: An Unconventional Challenge to the AML/CFT Regulators?" 21(3) *Journal of Financial Crime* 249-263 at 255.
57 Dostov & Shust (2014) at 255.
58 Dostov & Shust (2014) at 255.
59 Dostov & Shust (2014) at 255.
60 Chiu I (2017) "A New Era in Fintech Payment Innovations? A Perspective from the Institutions and Regulation of Payment Systems" 9(2) *Law, Innovation and Technology* 190–233 at 193.
61 Chiu (2017) at 193.

money cannot be traced.[62] With virtual currencies, there is no such protection,[63] which is a lamentable situation given that files stored on a computer can be subject to cyber-attack.[64] The point is that anonymity is not always a positive attribute for launderers and carries inherent risk. These arguments, however, do not diminish the value of or demand for anonymity by launderers as, with the growing intrusion of regulatory demands for information, decentralised currencies may be the future. However, for now this does not seem to be a measure of competition with other payment options.

Launderers also want to ensure profitability from their illegal ventures. They do not want a fluctuating currency as a form of payment, exchange or even a store of value. Because of its speculative nature, Bitcoin has not received mass acceptance. For this reason, JPMorgan refers to cryptocurrencies as a bad form of money.[65] This may be attributable to the high volatility cryptocurrencies in comparison with fiat currency. For instance, whilst the pounds to dollar rate has remained around £1 to $1.35 for over seven years, the Bitcoin to dollar rate has moved from $600 in September 2016 to $17 900 by December 2017, and by February 2018, it had fallen by 50%.[66] This instability reveals the confidence crisis that accompanies cryptocurrencies and their inability to compete with fiat currency as a form of payment, exchange or value through financial institutions or underground banking. Fiat money provides a generally stable exchange rate and has uniform value across the economy. Conversely, the transaction costs involved in laundering through Bitcoin is relatively lower. Whilst internet payment comes with regulatory burdens, even for simple utility bills, this is not the case with Bitcoin. The rational launderer thus is presented with a dilemma: although Bitcoin does not provide stability (which may be positive in instances where the prices escalate), it does provide reduced transaction costs. The option chosen would depend on the risk appetite of the launderer.

Bitcoin's competitive advantage over other payment options, particularly in West Africa, might lie in its offline presence. For instance, Swiss golden and MMM,

62 Chiu (2017) at 193.

63 Bohme R, Christin N, Edelman B & Moore T (2015) "Bitcoin: Economics, Technology and Governance" 29(2) *Journal of Economic Perspectives* 213–238 266.

64 Walch A (2015) "The Bitcoin Block Chain as Financial Market Infrastructure: A Consideration of Operational Risk" 18 *Legislation and Public Policy* at 837-893 at 837.

65 RT (17 February, 2018).

66 Cheng E (5 February 2018) "Bitcoin Continues to Tumble, Briefly Breaking Below $6,000" *CNBC*, available at https://www.cnbc.com/2018/02/05/bitcoin-drops-more-than-14-percent-to-below-7000.html (visited 21 March 2019).

two online Ponzi schemes, were successful partly because of their offline access.[67] Dostov & Shust argue that for cryptocurrencies to be as self-sufficient as cash or other payment instruments, they must have acceptability online and offline.[68] For now, the use of cryptocurrencies offline is limited to merchant ATMs or trade through cash. Additionally, their dominant online trade is not usually in payment form, but in exchange form,[69] indicating that their acceptability is confined to the virtual world, which possibly deters launderers.

Moreover, whilst the complexity of Bitcoin seemingly is attractive for launderers, customers have complained of difficulty in understanding how the cryptocurrency operates. Baur *et al* note that, of their sample size, only one interviewee agreed that Bitcoin was self-explanatory, whereas others mentioned the need for training to understand how the mobile wallets work.[70] Cryptocurrencies were perceived to be too complex to be understood by users and merchants — a hindrance that discouraged its use.[71] Spenkelink's findings are similar to those of Baur *et al*.[72] Consumers still focus on convenience, particularly regarding offline stores which constitute a space where cryptocurrencies operate sporadically. For this reason, Baur *et al* argue that credit cards, PayPal and other payment services will remain the popular online and offline payment options. Projections, however, indicate that although currently a niche area, Bitcoin is seen as the future because of the interest it is attracting.[73]

The literature indicates that whilst Bitcoin does indeed provide some advantages for launderers, there are hindrances to its competitive ability to displace other laundering options. Therefore, contrary to widely held perceptions, Bitcoin is not yet a technologically disruptive laundering tool. However, it does hold the potential to become disruptive. Given the myopic focus on CDD in West African countries, their current legal framework is inadequate to address the identity issues pertaining to Bitcoin. Accordingly, there is a need for evolution to ensure the continued relevance of the law in the light of technological innovations.

---

67 *The Cable* (3 August 2017) "MMM Returns to Nigeria, Adopts New Strategy to Woo Nigerians", available at https://www.thecable.ng/mmm-returns-adopts-new-strategy-to-woo-nigerians (visited 21 March 2019).

68 Dostov & Shust (2014) at 255.

69 Dostov & Shust (2014) at 255.

70 Baur *et al* (October 2015).

71 Baur *et al* (October 2015).

72 Spenkelink H (2014) *Identifying Factors that Influence the Adoption of Cryptocurrencies from a Multiple Stakeholder Perspective* (Unpublished Master's Thesis, University of Twente, The Netherlands).

73 Van Alstyne M (2014) "Why Bitcoin has Value" 57(5) *Communications of the ACM* 30-32 at 31.

4 LEGAL DISRUPTION?

The concept of legal disruption is significantly different from financial innovation disruption. According to the OECD report on Regulatory Reform and Innovation, legal disruption occurs when "technical change makes certain regulations obsolete and inefficient".[74] This happened with the advent of mobile technology[75] and, quite recently, with the advancements in payment technology underpinned by blockchain. Regulation of financial institutions and products traditionally were focused on investment portfolios, accounting and reporting practices, deposit insurance use and services offered to consumers.[76] These institutions were restricted in the services they could provide, hence their focus on consumer and commercial loans, savings and current accounts, or mortgages.[77] Also, interest rates, securities trading, foreign exchange transactions and capital movements were regulated at a micro and macro level.[78]

The advent of technology has occasioned changes in service delivery and payment options — transforming financial operations at the national and international level but with limited regulatory response. Like telecommunications, payments are becoming more immediate and anonymous, with implications for bank regulations and legislation. However, experiences regarding technological advancements, such as cyber law and online trading or bullying, have shown that it is always difficult for law to catch up with or understand technology.[79]

The slow pace of legal evolution in response to technological innovations may be appreciated by scrutinising the approach of West African countries to Bitcoin use. The responses of these countries may be classified into a protective approach, a cautious approach and a combination of protective and cautious approaches. Countries which have adopted the protective approach have placed a

74 OECD "Regulatory Reform and Innovation", available at https://www.oecd.org/sti/inno/2102514.pdf (visited 21 March 2019).

75 Whitfield B "Four Industries Affected by Mobile's Disruptive Technology" *Mobile Business Insights*, available at https://mobilebusinessinsights.com/2017/04/four-industries-affected-by-mobiles-disruptive-technology/ (visited 10 January 2019).

76 OECD "Regulatory Reform and Innovation".

77 OECD "Regulatory Reform and Innovation".

78 OECD "Regulatory Reform and Innovation".

79 Maney K (31 October 2015) "Law Can't Keep Up with Technology … and That's a Very Good Thing" *Newsweek Magazine*, available at https://www.newsweek.com/2015/11/13/government-gets-slower-tech-gets-faster-389073.html (visited 21 March 2018).
Signficantly, no West African country currently has a ban on Bitcoin. Namibia is the only country with such a ban. See Ecobank Research (1 August 2018) "Middle Africa Briefing Note", available at https://cdn.crowdfundinsider.com/wp-content/uploads/2018/08/Middle-Africa-Briefing-EcoBank-Note-Digital-African-crypto-regulation-August-2018.pdf (visited 19 January 2019).

total ban on trade in cryptocurrencies and criminalised their use.[80] This stance is taken irrespective of the recognition of blockchain as a facilitator of data management and storage through distributed ledgers.[81]

Nigeria took this step initially with a Central Bank regulatory circular which required financial institutions not to "use, hold, trade and/or transact in any way in virtual currencies".[82] Acknowledging later that an outright ban would stifle innovation, the Nigerian regulator resolved to rescind the prohibition and adopt the cautious approach.[83] Countries tend to adopt the cautious approach when they are conflicted about whether cryptocurrencies should be allowed to engineer technological innovation or should be regulated strictly to protect consumers. This approach permits persons and institutions to deal with cryptocurrencies at their own risk, pending substantive regulation.[84] Ghana has adopted the cautious approach, stating that cryptocurrencies are not licensed because its laws currently are unable to regulate digital forms of money. Ghana, though, is leading the adoption of blockchain in real estate transactions.[85] This is also the case with Sierra Leone, where a nationwide digitalisation programme is focused upon making West Africa the continent's first "Smart Country" through partnerships with blockchain companies.[86] Interestingly, in the 2018 Sierra Leone elections blockchain technology was used to tally votes in some regions, with the aim of improving transparency.[87] Yet, unlike to Ghana, its Central Bank has remained silent on Bitcoin regulation. Whilst Ghana's regulation is framed in terms of a protective-cautious approach which allows innovation flourish within this space, Sierra Leone's approach illustrates an aversion to Bitcoin in payment exchanges.

---

80 Mapp & Mwaita (6 July 2017).

81 Mapp & Mwaita (6 July 2017).

82 Central Bank of Nigeria (12 January 2017) "Circular to Banks and Other Financial Institutions on Virtual Currency Operations in Nigeria", available at https://www.cbn.gov.ng/out/2017/fprd/aml%20january%202017%20circular%20to%20fis%20on%20virtual%20currency.pdf (visited 10 March 2019).

83 Central Bank of Nigeria (12 January 2017).

84 Chuba C (9 August 2017) "Why Nigeria Has not Adopted Bitcoin Technology — CBN" *Today.ng*, available at https://www.today.ng/technology/internet/nigeria-adopted-bitcoin-technology-cbn-2575 (visited 21 March 2019).

85 Larnyoh MT (16 March 2018) "Ghanaian Banks Resist the Use of Cryptocurrency" *Pulse.comgh*, available at https://www.pulse.com.gh/news/business/ghanaian-banks-resist-the-use-of-crypto-currency-id8127392.html (visited 9 march 2019); Aitken R (5 April 2016) "Bitland's African Blockchain Initiative Putting Land on the Ledger" *Forbes*, available at https://www.forbes.com/sites/rogeraitken/2016/04/05/bitlands-african-blockchain-initiative-putting-land-on-the-ledger/ (visited 10 March 2019)

86 Ecobank Research (1 August 2018).

87 Ecobank Research (1 August 2018).

The caution of certain West African countries sometimes is expressed through regulatory silence. Member countries of the West African Economic and Monetary Union (UEMOA) — Benin, Burkina Faso, Ivory Coast, Guinea-Bissau, Mali, Niger, Senegal and Togo — share a central bank, the Central Bank of West African States (BCEAO). The BCEAO has denied reports that it attempted to launch a regional digital currency in 2017.[88] Quite interestingly, at the country level, the governments of these countries yet have to make a statement or take a public stance on the legality or otherwise of cryptocurrencies.[89] Silence may be indicative of a "wait and see" approach to regulating Bitcoin, as these countries are apprehensive about the potential risks associated with its use.[90] It does seem that, generally, African countries are waiting for global regulatory bodies or neighbouring countries to pronounce regulatory strategies before they do — to enable them transplant and learn from the mistake of others.

Countries which adopt the protective or cautious approach usually frame their responses within the context of AML laws and CDD requirements, as opposed to the broader picture of innovation.[91] Although done with the aim of countering money laundering, these responses do not address the imperfect knowledge of identities. For instance, the warning issued by the Central Bank of Nigeria (CBN) came amid growing fears that members of the public who are not tech savvy may be exposed to the risks of fraud and exploitation. Accordingly, the CBN directed financial institutions on AML requirements and compliance strategies. The evolution of Bitcoin, however, restrained the application of the law to regulate illicit financing through this structure. This is apparent from the steps taken by the CBN to address the perceived use of Bitcoin for illicit funding.

On 12 January 2017, the CBN issued a circular to Banks and other Financial Institutions on Virtual Currency Operations in Nigeria.[92] This circular banned cryptocurrencies, recognising the money laundering risk posed by them. The CBN

88 Ecobank Research (1 August 2018).

89 This is also the position with Cape Verde and Guinea. Senegal is an interesting case because, although the government has remained silent on the legality of cryptocurrencies, it was the first country in Sub-Saharan Africa to launch a digital currency in 2016. This virtual currency was tied to the country's legal tender, the CFA Franc. However the BCEAO distanced itself from this currency in 2017. Still, Senegal's banking system remains open to innovation. See Ecobank Research (1 August 2018)

90 Ecobank Research (1 August 2018).

91 In Cameroon, there is a slight variance as its framework regulation titled, *Regulation No 01/11-CEMAC/UMAC/CM — On the Use of Electronic Money*, outlines how electronic money can be used by the unbanked population in the region. This allows Cameroonians to transact with cryptocurrencies. Additionally, the Cameroonian government has tested the digital currency, demonstrating a willingness to engage with innovations in this space.

92 Central Bank of Nigeria (12 January 2017).

required that cryptocurrency exchangers have effective anti-money laundering controls that enable them comply with CDD and transaction monitoring criteria. More importantly, the circular empowered banks and other financial institutions to break off relationships with customers who are virtual currency exchangers and do not have adequate AML controls, and to report suspicious transactions by such customers to the Nigerian Financial Intelligence Unit (NFIU). Also, the circular reiterated that cryptocurrencies are not legal tender and that any bank or institution which engages in such business does so at its own risk.

The circular showed the CBN's recognition of the operationalisation of the Bitcoin trade. Its currency exchangers, however, were not prohibited from operating legitimately in Nigeria as long as they complied with the AML legislative requirements. By proclaiming that Bitcoins are not legal tender in Nigeria, the CBN evinced hesitation to allow cryptocurrencies a free reign while opting for an indirect way of regulating them.[93] Indirect regulation was adopted because regulating Bitcoin directly would be accepting that it is a legal tender. The Nigerian Federal Government has the exclusive constitutional right to coin money for the nation, regulate the value of the nation's coin, and prosecute anyone that impinges on this right. Bitcoin is decentralised, it can neither be coined nor have its value determined by the Nigerian Government.[94] Consequently, it is considered illegitimate.

The illegitimacy of Bitcoin disrupts the existing law as the evolution of the currency, coupled with the imperfect knowledge of identity it presents, makes the law somewhat inefficient. Recognising this deficiency, in February 2018 the CBN issued a press release to the general public which stated categorically that cryptocurrencies are not legal tender and anyone trading in it does so at his or her own risk, without the protection of the law.[95] This press release absolves the government of all responsibility should a Bitcoin deal go bad and transfers the burden of ensuring proper due diligence and risk management to the individual. To

93 Oyebode D & Shittu R (7 March 2018) "Evaluating the Central Bank of Nigeria's Directive on Cryptocurrency" *LinkedIn*, available at https://www.linkedin.com/pulse/evaluating-central-bank-nigerias-directive-damilola-a-oyebayo/ (visited 21 March 2019).

94 The likelihood of Bitcoin being confused with Nigeria's legitimate currency is quite low. The CBN, through a law passed by the National Assembly and assented to by the president of Nigeria, could restrict its use under clause 15 of the Exclusive Legislative List of the Constitution of the Federal Republic of Nigeria 1999 (as amended) which gives the Federal Government powers concerning currency, coinage and legal tender.

95 Central Bank of Nigeria (28 February 2018) "Press Release: Virtual Currencies not Legal Tender in Nigeria – CBN", available at https://www.cbn.gov.ng/Out/2018/CCD/Press%20Release%20on%20Virtual%20Currencies.pdf (visited 21 March 2019).

ensure robust regulation of Bitcoin, the government may decide to legislate on it or ban it outright. However, these attempts likely would be ineffective as the decentralised nature of the currency hinders national regulation. As an alternative, the government may decide to provide licences to exchangers as a means of regulation.[96] More strategically, government-backed cryptocurrencies may be created, but their sustainability may be questionable.[97]

The shortcoming of legislation may be perceived from the AML laws of West African countries. The Nigerian Money Laundering (Prohibition) Act of 2011 (MLPA), like the AML laws of other West African countries, seeks to provide financial institutions with sturdier tools to combat economic crimes. It was enacted in the light of GIABA's report which indicated that Nigeria's AML regime did not meet international standards.[98] The MLPA has expanded the scope of money laundering offences and provided for enhanced due diligence measures.[99] Also, financial and non-financial institutions are to verify beneficial owners using reliable data.[100] These requirements, which bestow a gatekeeping responsibility upon financial and non-financial institutions, enhances the capability of regulatory bodies to combat economic crimes more robustly.

The MLPA contains specific requirements limiting the amount of money that can be transferred outside a financial institution to $13 900 for individuals and $27 800 for a body corporate.[101] These limits are aimed at ensuring that any transfers exceeding them are done through a medium that would record the transactions. Financial and non-financial institutions which receive amounts above the statutory threshold are required to carry out robust CDD.[102] Such CDD requires an evaluation and verification of the customer's identification, including reasonable measures taken to uncover the beneficial owner. CDD eases the process of reporting suspicious transactions to the NFIU.

An application of these legal requirements to cryptocurrencies reveals certain inconsistencies. Three instances are worthy of consideration. The first relates to transactions within the Bitcoin ecosystem. Where the owner of two

96 Oyebode & Shittu (7 March 2018).

97 This is due largely due to the cost and energy implications. Cameroon tried it but stopped for these reasons. See Ecobank Research (1 August 2018).

98 GIABA (May 2015) *Seventh Follow Up Report: Mutual Evaluation, Nigeria*, available at https://www.giaba.org/media/f/932_7th%20FUR%20Nigeria%20-%20English.pdf (visited 10 March 2019)

99 Section 3(1)(a) of the MLPA of 2011.

100 Section 3(1)(a) of the MLPA of 2011.

101 Section 1(a) & 1(b) of the MLPA of 2011.

102 Section 3(1)(a) MLPA of 2011 as read with Section 1(a) & 1(b).

Bitcoins, valued at $2 in 2010 but currently is worth $24 986, seeks to sell his Bitcoins to another user within the network, he would be deemed in breach of the MLPA. This is because Bitcoins operate outside the sphere of financial institutions. Secondly, where Bitcoins are exchanged for valid currencies, particularly if the transfer is done through a financial institution, the latter may decide to de-risk the operator for not showing evidence of CDD or reporting as required by the CBN. In these two instances, the underlining issue is whether Bitcoin is a legal tender. As previously established, it is not. Therefore, the applicability of the MLPA is restricted. If the MLPA applies, it may undermine the benefit of anonymity which Bitcoin provides its users.

The limitation of the MLPA is more glaring in the third instance — where CDD cannot be carried out. Regular CDD becomes more complex with Bitcoins. As explained above, the payment process of Bitcoins relies on aliases and encrypted codes, which are not associated with the true identity of the owner. This circumstance suggests that attempts to carry out CDD would be futile, thereby signposting the inapplicability of the MLPA. There appears to be a grey area in the law which is attributable largely to the decentralised nature of Bitcoin.

The shortcoming of the approaches adopted by West African countries to addressing the imperfect knowledge of identities requires that law incorporate elements of technology. The demands of technology force law to start reconsidering its relevance, by seeking to understand the Bitcoin processes prior to issuing an outright ban. Currently, in the absence of targeted law, policy or guidance, there are only warnings from central banks which are inadequate for addressing the issue. The question, then, is how Bitcoin may be regulated in a manner that does not stifle innovation whilst protecting the increasing customer base in West Africa?

5 THE WAY FORWARD

The increasing use of Bitcoin in a networked region presents a significant challenge to regulatory capacity to cover contemporary circumstances. Difficulties abound in drafting legislations in an area fraught with uncertainty and complexity. The rigidity of a rules-based approach is inapplicable here. By contrast, a principle-based approach which offers guidance and sets best practices for Bitcoin operators would offer clarity and protection to users, whilst minimising potential for laundering. For effectiveness, the guiding principles should be domesticated to take into consideration language differences and the socio-economic background of users. Also, they should provide clarity for users and resolve asymmetries between operators and customers.

In the absence of a principled regulatory framework which comprehends Bitcoin operations, including their ongoing evolution and loopholes for laundering, there might be continued reliance on old laws and regulations. These laws and regulations are incapable of addressing Bitcoin anonymity and the money laundering risk. This is because, currently, Bitcoin works outside the regulatory scope of West African countries and the existing rules cannot ensure consumer protection or limit laundering. A new regulatory framework is required which, eventually, may have to cross jurisdictional borders to ensure that all Bitcoin operators are subject to the same standards.

6 CONCLUSION

Arguments abound on the disruptive nature of Bitcoin to laundering processes, which disruption stifles technological innovation in West African countries. This paper has attempted to deconstruct this position and finds that Bitcoin is not yet technologically disruptive to money laundering processes, although it has the potential to be. A cost-benefit analysis shows that a rational launderer who aims to maximise profit indeed may suffer loss through reliance on Bitcoins. This is due largely to the volatility of the cryptocurrency and the seeming anonymity which it confers. However, given that no study yet has quantified the volume of transactions through Bitcoin linked to laundered funds, it cannot be argued affirmatively that Bitcoin is disruptive to existing laundering mechanisms.

This paper finds that the disruption which Bitcoin poses is of a legal kind, as the current laws and regulations in West African countries are inadequate to addressing Bitcoin's anonymity issue in particular. The current CDD regime would be inapplicable as it depends upon the identity of users. Evaluation of the approach taken by West African countries to Bitcoin indicates that current regulations are obsolete in relation to Bitcoin technology. Consequently, there has to be a fundamental change in the law, aimed at accommodating innovation, to ensure the continued relevance of the law as regards innovative laundering processes. It is submitted that a principle-based regulatory approach is needed if West Africa is to cope with the complexity and lack of clarity presented by Bitcoin and other cryptocurrencies.