REPORT OF THE SECOND ROUNDTABLE DISCUSSION ON CRYPTOCURRENCY AND BLOCKCHAIN REGULATION IN UGANDA HELD ON 6TH JULY 2017

Full report

ABSTRACT

The Second Round table on developing of Principled Guidance for the regulation of crypto currencies in Uganda took place on the 6th July 2017 at the United Nations African Institute for the Prevention of Crime and the Treatment of Offenders (UNAFRI) in Naguru, Kampala. The participants developed principled guidance on the regulation of cryptocurrencies based on a co-regulatory model.

Mapp

Dr. Maureen Mapp, Convenor and report author.
Mr. Patrick Mwaita- (UNAFRI) programme organiser.
The event was co-sponsored by UNAFRI and the University of Birmingham Law School.

Table of Contents

Report of the Second Roundtable discussion on Cryptocurrency and Blockchain regulation in Uganda (6th July 2017) 3

Background 3

Problems with current regulatory responses to cryptocurrency use 4

Summary of agreed principled guidance 5

PANEL 1: CRYPTOCURRENCY AND THE BLOCK CHAIN: WHY REGULATE? 7

Opening Statement by Mr. John Kisembo, Director of UNAFRI 7

Regulating disruptive payment technologies in Africa: Dr Maureen Mapp (Convenor, Birmingham Law School, University of Birmingham) 8

Cryptocurrency regulation in Africa 14

How should we regulate disruptive payment technologies? 15

Principled versus rules based approaches to regulation 16

Key note address by Mr Stephen Mulema, Director of Financial Markets, Central Bank of Uganda 17

Cryptocurrency investment in Uganda: Mr Ivan Kintu, Cryptocurrency Evolution Ltd 19

Fintech require clarity from regulators 21

PANEL 2: INFORMATION TECHNOLOGY, THE JUDICIARY 22

National Information Technology Agency: Mr Emmanuel Mugabi and Ms Caroline Akello-Mugisha 22

NITA-U policy considerations 22

Judicial Training Institute: Dr. Gladys Nakibuule-Kisekka, Deputy Director Law Reporting and Research and Training 24

Recommendation 25

PLENARY SESSION 1 25

Cryptocurrency inflationary tendencies 25

Taxation - use of current laws to prevent tax evasion 25

Protecting the Public interest 26

PANEL 3: POLICING, COMMUNCATIONS, AND INTELLIGENCE MONITORING 27

Policing Cryptocurrency fraud: Mr Dan Munanura, Assistant Commissioner of Police and Director, Electronic and Counter Measures, Uganda Police Force 27

Recommendation 28

Uganda Communications Commission: Mr Julius Mboizi, Senior Officer, Legal Affairs 28

Recommendations 29

Financial Intelligence Agency (FIA-Uganda): Ms Esther Kagira-Aikiriza, Manager, International Relations and Strategic Analysis 29

FIA AML/CFT policy developments 30

Recommendations 30
PLENARY SESSION 2 31
Challenges to fiat currency 31
Developing an institutional arrangement around the peer to peer networks 31
Legitimisation of cryptocurrency 32
Privacy – an ethical dilemma 32
Cultivating a collaborative co- regulatory approach 32
Managing Risk 32
PANEL 4: SOCIO CULTURAL LEGITIMACY OF REGULATION 33
Drafting socially relevant cryptocurrency regulation: Dr. Anthony Kakooza, Dean of the Faculty of Law, Uganda Christian University, Mukono (UCU) 33
Recommendations 34
Legal challenges to regulating cryptocurrency: Dr Ronald Kakungulu- Mayambala, Senior Lecturer, Makerere University School of Law, Kampala 34
Recommendation 36
Socio-cultural transformation' of regulation: Dr Maureen Mapp, Birmingham Law School, University of Birmingham 36
Recommendation 39
PLENARY SESSION 3 39
Keeping pace with changing technology 39
Data sharing 39
Choice of terminology for regulation 40
Increasing smart phone ownership 40
Making customary law applicable 40
Sociology of regulation 40
Closing Speech: Mr John Kisembo, Director of UNAFRI 41
Declaration on Fundamental Principles on the regulation of cryptocurrencies and the Blockchain (Digital Ledger Technologies) in Uganda and its Follow Up 43
Preamble 43
ANNEX 46
FOLLOW-UP TO THE DECLARATION 46
PRINCIPLES 46
Participants at the Second Round Table (6th July 2017) 50

Report of the Second Roundtable discussion on Cryptocurrency and Blockchain regulation in Uganda (6th July 2017)

Background

The second round table on the development of Principled Guidance for the regulation of cryptocurrencies in Uganda took place on the 6th July 2017 at the United Nations African Institute for the Prevention of Crime and the Treatment of Offenders (UNAFRI) in Naguru, Kampala. The event aimed to consolidate the gains of the first RoundTable (held on the 7th July 2016) at UNAFRI. The purpose of the first round table was to engage policy makers, academics and regulators in critical discussion on the possible regulation of cryptocurrencies, to exchange experiences, and to develop instructive guidance based on principles of a multi-disciplinary nature.

The first and second roundtables arise from partnership between UNAFRI and Dr. Maureen Mapp of the Birmingham Law School, University of Birmingham which further the mandate of UNAFRI to offer technical assistance to African States in the development of policy and of legislation on the regulation of disruptive technology. The roundtables draw on external support from research done by those working in academia and other bodies; and engage policy makers, financial regulators, academia and cryptocurrency businesses in critical discourse on the complex legal, socio cultural and policy issues of regulating crypto currencies and the implications of regulation for the wider meanings of currency.

Participants to the second round table were drawn from cryptocurrency enthusiasts and businesses; from financial regulators including the Central Bank of Uganda, and other regulators like the National Information Technology Agency, the Uganda Communications Commission, and the Financial Intelligence Agency. Also represented were the Uganda Police Force, the Uganda Law Reform Commission, the Judicial Training Institute, the Uganda Revenue Authority, and individual researchers and from academia. Participants agreed a number of recommendations: a report of the proceedings of the Roundtable on the impact of cryptocurrency on investment and trade in Uganda, and the need for principled guidance in line with the commitment of participating regulators to promote technological neutrality, co-regulatory approaches, socio-cultural legitimacy, consumer protection and ethical practices that were fair, non-discriminatory and non-deceptive, and were underpinned by the principle of legality. In order to supplement Uganda's largely rules based approach to regulation and to make it relevant to Uganda's emergent tech enabled economy, the principles would be integrated into comprehensive policies like the monetary policy, into strategies like the digital strategy, and into awareness-raising measures.

To assist in the development of principled guidance, the participants drew on the Report of the first Round table (Kampala 2016), and the Report of the Commonwealth Working Group on Virtual Currencies (2016). In its survey on the prevalence of virtual currencies in the commonwealth countries including in Uganda, the Working Group established that many nation states had not adopted a specific approach to the regulation of virtual currencies,

although it was evident that the currencies were in use in those countries. The recommendations of the Working Group included the determination on the legality of virtual currencies, awareness raising about virtual currencies including the risks, the adaptation of existing legal frameworks or enactment of new laws on the use of virtual currencies, capacity building and the creation of conducive environments for the development of virtual currencies.[1] Participants also drew on regional conventions like the African Convention on Cybersecurity and Personal Data Protection (2014), the African Charter on Human and Peoples' Rights (1981); on existing legislation like the Uganda Constitution, the Value Added Tax Cap 349, and 'soft law' like the Bank of Uganda Consumer Protection Guidelines 2011.

Problems with current regulatory responses to cryptocurrency use

The expanding use of disruptive payment technology in the modern networked Africa constitutes a significant challenge to the regulatory capacity to respond to contemporary circumstances. While the importance of cryptocurrency and its underlying technology- the Blockchain, are tentatively recognised in the policy sphere as a cost effective method of enabling micropayments in African economies, the lack of regulation presents unique challenges. The problem can be summarised as a communication gap between lawmakers, policy-makers, regulators and the crypto currency businesses about the socio-cultural, legal, economic and political effects of this emergent cryptocurrency environment. Without a principled regulatory approach to plug this gap, the development of policy and laws, law enforcement, and the adjudication process could be based on antiquated rules that may not deal with important conceptual and practice based issues. These issues include the legal status of cryptocurrency; tax liabilities, the risk of cybercrime- including the exploitation of vulnerabilities in technology to hold financial systems at ransom and exploiting those consumers who fail to use the technology correctly. There is also the lack of effective consumer protection, and the arbitrary use of discretionary power by regulatory bodies. These issues are of concern given the move by Fintech start-ups and some financial regulators to offer more cryptocurrency and Blockchain based products to the Africa based consumers. The Kenya Capital Market Authority for example has launched the M Akiba bond on the Nairobi Stock exchange-the first mobile traded government bond of its kind in the world to use the Blockchain.[2] Other products include cryptocurrency exchanges like Bitreco- a Uganda based Bitcoin exchange.

Unlike fiat currency (the Uganda shilling) whose creation and use is regulated and limited by the Central Bank of Uganda, there is no such limitation on the acquisition and use of cryptocurrencies as Uganda has not formally appreciated the nature and impact of virtual currencies. Even so, the recent warning from the Central Bank of Uganda (14th February 2017) to the public against investment and conducting business using Onecoin and similar crypto currencies like Bitcoin and Litecoin underscores the vulnerabilities that consumers face, and

[1] Report of the Commonwealth Working Group on Virtual Currencies, *Commonwealth Law Bulletin* (2016) 42 (2) 263-324.

[2] https://www.african-markets.com/en/stock-markets/nse/kenya-m-akiba-mobile-bond-starts-trading-at-nairobi-securities-exchange. More information about the working of the bond can be found at http://www.m-akiba.go.ke/.

the risks posed by the unregulated use of cryptocurrencies in Uganda. The Central Bank's warning comes amid growing fears that unsuspecting members of the public who are not tech-savvy may be exposed to risks like fraud and to exploitation, yet they might not know how to confront these risks and the fallout from exploitation.

In order to address these challenges, the second round table debated the need for regulation, the appropriate approach to be adopted, and questioned whether the draft guiding principles that were developed at the first Round Table event in July 2016 could help give clarity to cryptocurrency and Blockchain based businesses and users in these six main areas**:**

1. Technological security, trust and risk assessment.
2. Policy approaches to regulating crypto currency and the Blockchain.
3. The legality of crypto currency including user rights, obligations of the state and of providers, consumer protection, and the promotion of ethical behaviour.
4. The applicability of existing legislative frameworks in areas such as taxation, insurance and proceeds of crime.
5. Investigatory, prosecutorial and judicial approaches to digital forensic models.
6. Engendering socio-cultural legitimacy; and the consideration of socio-cultural issues surrounding consumer behaviour among poor, rural and illiterate African communities when using smart technologies.

This report documents the discussions regarding the 'lived' experience of cryptocurrency businesses and of financial regulators including the Central Bank of Uganda in dealing with cryptocurrencies, and highlights the prospects and challenges of developing any sort of regulation- whether principled or rules based, of cryptocurrency and the Blockchain in Africa. This report contains the responses to the questions posed above. Another event is scheduled to take place in 2018.

While acknowledging the difficulty in achieving a holistic conceptual definition of cryptocurrency due to the variety to approaches internationally, the Round tables used the generic definition of the Financial Action Task Force (FATF) [3] of cryptocurrency as a type of decentralised virtual currency which lacks a central authority. Virtual currencies can be viewed as a digital representation of value that can be traded, function as a medium of exchange, a unit of account and/or a stored value, but has no legal tender status in any jurisdiction. An initial coin offering is referred to as private means to raise funds for a new crypto-currency business via the purchase of tokens - known as coins – that are issued in return for virtual currencies, like Ethereum or Bitcoins.[4]

Summary of agreed principled guidance

The participants to the Second round table agreed to the following principles to guide any policy and regulatory measures which are elaborated upon in the *Declaration on Fundamental*

[3] FATF, *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*. Available at http://www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html.
[4] Hermann Elendner, Simon Trimborn, Bobby Ong, and Teik Ming Lee, "The cross-section of crypto-currencies as financial assets: An overview" Working Paper 2016, University of Humboldt https://www.econstor.eu/bitstream/10419/148874/1/870165852.pdf

Principles on the Regulation of cryptocurrencies and the Blockchain (Distributed Ledger Technologies) in Uganda (at the end of the document).

1. There is need for regulation that offers clarity to both the investor in cryptocurrency and the fintech start-up or business. Regulation should offer protection to the consumer and prevent the use of cryptocurrency to engage in illegal activities like tax evasion or money laundering.
2. Conceptual clarity is required surrounding the definition of currency and money in existing law. These definitions can then be adjusted to include forms of cryptocurrencies in the law. Clarity and consistency is also needed on the categorisation of cryptocurrency whether as a security, a commodity, property, currency, or something else.
3. The Blockchain ought not to be regulated, pending a wider benefit –risk analysis.
4. Terms and conditions for the use of cryptocurrency should be simplified and translated into local languages so that consumers/investors who enter into these transactions can better understand their obligations, rights and liabilities. This is more so when dealing with the rural poor and illiterate or semi-literate customers.
5. In order to avoid over regulation and confusion about compliance requirements, the government should decide on the key regulator (s) from the range of potential financial regulators including the Central Bank of Uganda, the Uganda Revenue Authority, the Uganda Communications Commission, National Information Technology Agency, Uganda Capital Markets Authority, and the Insurance Regulatory Authority.
6. Regulation should be cross-jurisdictional in nature through cross border cooperation mechanisms including mutual legal assistance so as to better coordinate investigations, monitoring, prosecutions and adjudication of this transnational cryptocurrency trade.
7. Technological neutrality should aim to regulate the service or product, but not the provider.
8. Public awareness is necessary in order for individuals and the general public to understand the benefits and risks of cryptocurrencies. In addition, a better understanding of way cryptocurrencies work can help inform future policies.
9. Policies need to achieve some form of harmonisation or functional equivalence among the interrelated policies like fiscal policies, monetary policies, taxation policies, Intellectual property policies, Information Communication Technology policies and the like. A risk based proportionate approach could best underpin policy and regulation in order to keep the services affordable to those on low incomes.
10. Policies and regulation should deal with the tensions between the attributes of cryptocurrency like lack of a centralised authority, decentralised ledgers, and pseudo-anonymity; and the regulatory requirements like Know Your Customer and Anti Money Laundering that are underpinned by the need for physical address of a business or natural persons, and a centralised authority.
11. Update existing laws to have a functional approach to digital forensics and analysis. This could include an application of traditional banking disclosure requirements and know your customer requirements to online activities. Equally, law revision should aim to resolve the contradictions and tensions between anti-money laundering laws, and consumer protection laws.

12. Cross-cutting capacity building programmes could enhance skills in the JLOS, among policy makers, legislators and regulators, working together with academia and with the business community.
13. Understanding socio-cultural issues surrounding consumer behaviour among the poor, rural and illiterate communities is important given that cryptocurrencies create a kind of cultural shock for these communities. The cultural shock may be because the medium of exchange is based on peer to peer networks and anonymity.
14. The issue of ownership and transfer of cryptocurrencies within localised communities ought to be appreciated by the regulators. Regulation should address questions surrounding how the transfer will happen; what happens to transfer in the case of an emergency or eventuality where the ownership has not been disclosed to third parties.
15. Maintaining the independence of (private) peer to peer transactions requires a careful management of regulations that address the risks associated with cryptocurrencies such as security, privacy and protection. Regulations should aim to build trust in these transactions. Creating a culture of secrecy around the operation of cryptocurrencies on the Blockchain may breed distrust among the communitarian societies where information is largely open. Trust may be achieved by having strong consumer protection regulations and secure record keeping.

PANEL 1: CRYPTOCURRENCY AND THE BLOCK CHAIN: WHY REGULATE?

Opening Statement by Mr. John Kisembo, Director of UNAFRI

In 2016, the first round table held at UNAFRI opened up discussions on cryptocurrencies as a result of the collaboration between UNAFRI and the University of Birmingham Law School. The collaboration brought together a cross-disciplinary panel of experts to address issues surrounding the regulation of cryptocurrencies and its underlying Blockchain technology including the applicability of currency as consistent with the wider meanings of currency. The composition of the second roundtable reflects the growing interest from a spectrum of experts whose work informs policy and legislation regarding a safe model of utilisation of cryptocurrencies.

At the first roundtable in 2016, cryptocurrencies were viewed as shrouded in mystery, with participants fearful yet eager to know more about it. Since then, people's understanding of cryptocurrencies has grown and so has its use as a medium of exchange for services and goods especially among the city folk of Kampala. On the 14th of February 2017, the Bank of Uganda issued a cautionary note to the general public against the continued use and dealing in cryptocurrencies. This note was a clear disclaimer on the part of the Central Bank in the face of imminent uncertainties and consequences arising from the lack of regulatory mechanisms and policy guidelines for the use of cryptocurrencies. Amazingly, the Ministry for Finance and Economic Development appear to have adopted a 'wait and see' approach to regulating a business previously dubbed a 'Dark Web invention' that has now taken root in the public domain. This lack of clarity from the Ministry, appears to mask a policy dilemma.

Indications are that the digital currencies are running parallel to the legal tender 'fiat' currencies. But what might happen in the near future? Indeed the warning from the Central Bank has caused a spate of genuine inquiries from the worried public some of which are reported in the social media and in the newspapers.[5]

This round table is a step forward in the search for appropriate intervention from the regulatory authorities-, one that is based on the sharing of expertise, knowledge, and ideas. This event should also help in de-mystifying the concept of cryptocurrencies and by the same token deliver the proposed intervention. Any prospective regulation of cryptocurrencies, ought to take into account the impact of these innovations on domestic policies, and on the legal, socio-cultural, economic and ethical environment. This event is significant as it feeds into the African regional efforts to address and to harmonise fiscal and related policies and to offer guidance on the imminent integration of such polices.

It is on record that Uganda is the first country to have multi stakeholder roundtable discussions on the possible regulation of cryptocurrencies in Africa.[6] Despite this progress, there are understandably those people who might still be sceptical about the use of these cryptocurrencies and may fear to explore the unknown. UNAFRI aims to expand the growth of knowledge and in this regard UNAFRI in collaboration with Birmingham Law School will continue to host discussions on the potential of cryptocurrencies to spur Africa's advancement in technology while simultaneously posing socio-cultural challenges to consumers and regulators alike.

Regulating disruptive payment technologies in Africa: Dr Maureen Mapp (Convenor, Birmingham Law School, University of Birmingham)

This second round table offers an opportunity for payment and investment technology businesses and start-ups (broadly termed here as 'Fintech') and regulators to have an open discussion on the ways in which regulatory authorities can provide a conducive environment in which Fintechs may test 'disruptive products such as Blockchain technology, big data and crypto-currency. Viewed as disruptive to traditional payment systems, emerging payment technological innovation offers both an "opportunity" and a "challenge" to African domestic financial institutions. Payment and investment technologies are driven by the exponential growth in mobile money and use of smart technologies in Africa. Studies show that mobile internet penetration in Africa was 23% in 2015 and there is evidence that mobile technology use contributes to social and economic development across the continent. In 2014, the mobile technology and service industry contributed 5.7% of the Gross Domestic Product (GDP) which was around one hundred and two billion United States dollars' (USD) worth of economic value. This figure is expected increase to more than one hundred and sixty six billion USD dollars

[5] Darious Nkwaibwe, "Who will save us from Ponzi Schemes, Letter of the Day, *Daily Monitor* 28th April 2017 (Uganda).
[6]Jamie Redman, "Uganda Considers Future Cryptocurrency Regulations" at https://news.bitcoin.com/uganda-future-cryptocurrency-regulations/. See also 'Africa expects big things from Bitcoin in 2017',http://www.businessworldghana.com/africa-expects-big-things-bitcoin-2017/ .

which is estimated to be about 8% of GDP by 2020.[7] The increased adoption of mobile and internet-based Blockchain technology is predicted to drive African states to create conducive environments for crypto-currency and Blockchain initiatives given that mobile money platforms like M-Pesa have opened up endless potential for cryptocurrency-based applications.[8]

Since 2009, when Bitcoin- the first cryptocurrency was created by a fictional Satoshi Nakamoto,[9] the cryptocurrency market worldwide has grown fourfold spanning a range of cryptocurrencies and investment ventures like the initial coin offerings. The market capitalisation of cryptocurrencies surpassed US$100 billion for the very first time in June 2017.[10] Despite this exponential growth, there is little information about the market capitalisation of cryptocurrencies in Africa given the difficulty of determining the geographical distribution of cryptocurrency users.[11] South Africa has the largest share of the African market, and the findings of the 2015 Commonwealth survey establish that at the unregistered, unofficial level that represents more of a consumer base, several individuals and small groups had adopted the Bitcoin- a type of cryptocurrency, as a mode of payment. For example, four Ugandan based online groups offered trade services in Bitcoin on Facebook; and more than 10 individuals/groups were registered as dealers and sellers on international cryptocurrency websites. At present there are several cryptocurrency businesses in Uganda, with one of them- Cryptocurrency Evolution Limited, represented here at this second Round table. [12]

The growing opportunities to revolutionise e-commerce for the benefit of the largely unbanked populations in Africa, appears to stem from having a technology that can be used on any smart device including on mobile phones. Here, cryptocurrency – a form of digital currency, can be stored in a digital wallet using encrypted techniques to regulate the generation of the units of currency, all the while operating independently of a third party or intermediary (like a Central Bank) that may intervene in the transactions. The relative anonymity of cryptocurrency transactions is viewed as a safety feature, as is its cryptographic protocol in which the owner has a private cryptographic key for use in their digital wallet and to move their funds via a digital signature onto the Blockchain. The Blockchain, which may be a public or private (decentralised) distributed public ledger of transactions, also offers its users trust that emanates from the process itself- real time validation of changes across the network, shortened transaction times, improved transparency and a potential reduction in transaction

[7] Global System for Mobile Communications Association (GSMA), *The Mobile Economy Sub Saharan Africa* 2015- https://www.gsma.com/mobileeconomy/archive/GSMA_ME_SubSaharanAfrica_2015.pdf.
[8] Bithub Africa, *Report on the African Blockchain Opportunity Crowd-Sale Campaign* available at http://bithub.co.ke/opportunity/?wpam_id=1).
[9] Satoshi Nakamoto "Bitcoin: A Peer-to-Peer Electronic Cash System" at https://bitcoin.org/bitcoin.pdf. Nakamoto's work was preceded by that of David Lee Chaum who invented electronic money, internet anonymity and 'digicash'- an e-money business.
[10] https://coinmarketcap.com/charts/.
[11] Garrick Hileman & Michel Rauchs, *Global Cryptocurrency Benchmarking Study* 2017, available at https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf
[12] The findings are in the Report of the Commonwealth Working Group on Virtual Currencies", *Commonwealth Law Bulletin* (2016) 42 (2) 263-324. The survey on Uganda was conducted by Maureen Mapp under the auspices of the Rule of Law Division of the Commonwealth Secretariat.

costs.[13] Some of the benefits of adopting the Blockchain in Africa include international remittances where companies like Remitano facilitate international transfers of money using Bitcoin through the use of its current Escrow platform in countries like Nigeria, and Kenya. Other potential uses are in the cyber insurance sector to verify transactions, deter frauds and manage risks.

Some policy challenges

Despite the growth opportunities in the Fintech sector, the lack of formal recognition of the growing consumer base in cryptocurrencies, and of the potential vulnerability of consumers, underlie the need for a careful consideration of policy and legislative issues that underpin any potential regulation. There is no law, no policy, no interpretive guidance, no opinion or strategy on the place for cryptocurrency and related investment vehicles in Uganda or in Africa generally. What exist are warnings from Central Banks such as that issued by the Central Bank of Uganda in February 2017. In addition, direct threats to cryptocurrency businesses; to consumers; as well as to the nation in the form of hidden resource costs, all require policy guidance and possible legislation.

From the business perspective, Fintech including cryptocurrency businesses need clarity regarding requirements for compliance, and for consumer protection. Fintech's concerns relate to the potential rise in compliance costs if legislation is put in place. There is also the cost to the business for ensuring transaction security and the security of data for all those involved in the payment process: issuers, consumers, merchants, and mobile telecom providers. The cryptocurrency may itself suffer a lack of resilience (volatility) if their market value drops due to regulatory clampdowns.

Cryptocurrency own limitations could affect its widespread adoption. For a start, the volatility of a cryptocurrency's exchange value against another currency, and changes like the impending hard fork (divergence in the Blockchain) may affect the stability of the cryptocurrency. There is the problem of scalability where the size of transitions are too big and complex to process quickly which could reduce the speed of transactions. Vulnerabilities in the technology like bugs in the code can enable the theft of cryptocurrency from an individual's digital wallet through hacking. The hacking can occur despite accounts and wallets having extra security like a two-factor authentication. Reports indicate that Parity- one of the world's largest digital wallet provider that enables cryptocurrency miners to store Ethereum (a cryptocurrency) was hacked with over 153,000 Ether, which is worth approximately $30 million US dollars, stolen in June 2017. With each hack is a real possibility that some may lose their investments as could happen to the MtGox investors in Japan where in 2014, approximately $350 million of Bitcoin was stolen by hackers. Equally, data security and data protection is at risk if companies/start-ups have not secured their customers data and the data is then hacked and sold on, or by businesses using data without obtaining express consent of users to process sensitive personal data. Where there is an append-only feature of a given Blockchain-

[13] For a more technical description of the more widely used cryptocurrency – the Bitcoin and their design see Satoshi Nakamoto, 2008, Glen Williams, David Gunn, Eduardo Roma and Bharat Bansa**,** **"**Distributed Ledgers in Payments: Beyond the Bitcoin Hype", June 13, 2016 at http://www.bain.com/publications/articles/distributed-ledgers-in-payments-beyond-bitcoin-hype.aspx, and Rainer Böhme, Nicolas Christin, Benjamin Edelman, and Tyler Moore "Bitcoin: Economics, Technology, and Governance", *Journal of Economic Perspectives* (2015) Vol. 29, No. 2, 213–238.

where information (data) uploaded onto it may be difficult to remove, this raises questions of consumer data privacy. We cannot overestimate the need for some sort of supervisory oversight given the security risks posed to users and to their data.

The lack of legitimate outlets in which to trade in cryptocurrencies may not only pose a barrier to the adoption of cryptocurrency, it may also lead to unscrupulous traders stealing from the unsuspecting public and demanding ransoms. This was the case of Ronald Nsubuga. In the video entitled *Bitcoin in Uganda - Empowering People*, Ronald a Kampala resident received a cash equivalent of Bitcoins from his sister in the United States of America, to pay his tuition fees.[14] Sadly, after the first successful transaction, Ronald was ripped off by the Kampala based Bitcoin merchant who disappeared with Nsubuga's tuition fees. Apart from individual loss like Nsubuga's, there is the growth of illegal use of cryptocurrency on the Dark Web as the currency of choice for the purchase of illegal guns, and drugs. Bitcoin is also the payment of choice for recent ransom malware incidents such as WannaCry and Petya. Countries like South Africa, Nigeria, Angola, Egypt, Mozambique, Tanzania, Niger, Morocco and Tunisia, were hit by Wannacry according to Kaspersky Lab and ransom payments demanded in Bitcoins.[15]

Notably, there is a 'hidden' resource cost of electricity for those who 'mine' cryptocurrency by using their computers to solve mathematical computations, and to check all monetary transactions, which in turn creates the cryptocurrency as a reward. The mining is done on computers that use electricity, but so do other activities like using electricity to power the devices like smart phones and the servers that are used for trade. Some like Sebastian Deetman predict that at the current growth rates in computing efficiency, the Bitcoin network could consume up to 15GW by 2020, which is equivalent to the consumption rate of Denmark in 2014. Earlier studies like that of O'Dwyer and Malone estimate the total electricity consumption of the Bitcoin network in early 2014 was comparable to that of Ireland (roughly 5GW).[16] These facts are significant given that electricity supplies ought to match the resource cost of maintaining the cryptocurrency network in terms of the national electric consumption. Uganda's access to electricity stands at 15% up from 7% (as of March 2017) - the equivalent of 601.1 MW.[17] While this level of generation of electricity is commendable, if electricity consumption of Uganda's cryptocurrency network outstrips supply, this could jeopardise a conducive environment for digitalising e-commerce.

The last major challenge for policy makers is at the level of fiscal policy. Even though it is unlikely that cryptocurrencies will pose an immediate threat to fiat currencies given the dominance of cash around the world, even in technologically advanced states like the United States of America (USA) and the United Kingdom the dominance of cash appears to negate

[14] The *Bitcoin in Uganda* video is available at https://www.youtube.com/watch?v=BrRXP1tp6Kw.
[15] Ismail Akwei, "Africa least hit by WannaCry ransomware cyber-attack" available at: http://www.africanews.com/2017/05/15/africa-least-hit-by-wannacry-ransomware-cyber-attack//
[16] Sebastian Deetman, "Bitcoin Could Consume as Much Electricity as Denmark by 2020" (2016) available at: https://motherboard.vice.com/en_us/article/aek3za/bitcoin-could-consume-as-much-electricity-as-denmark-by-2020. Karl O'Dwyer and David Malone, "Bitcoin Mining and its Energy Footprint", ISSC 2014 / CIICT 2014, Limerick.
[17]Uganda's Electricity Sector Overview (March 20197) at http://www.era.or.ug/index.php/sector-overview/uganda-s-electricity-sector. Uganda intends to increase access to the national grid to 80% by 2040- *Uganda Vision 2040*.

a threat to a centralised authority (like a bank) that transfers value, records and verifies transactions centrally. Even so, the very nature of cryptocurrencies pose a threat to the centralised transactions because of their decentralised features. For example, it is difficult for centralised authorities to control transactions that are recorded on a private Blockchain and distributed via peer to peer networks. This may seem like a moot point now, but as cryptocurrencies gain value, they may begin to compete with fiat currencies.

Global Regulatory trends

Regulation of cryptocurrency at the global level started pre 2015 around 2009, when Satoshi Nakamoto created the Bitcoin as a peer to peer currency. At that time, there were concerns regarding the threat posed by Bitcoin to the stability of the economy as well as its legality vis-a-vis fiat currency. Other questions related to the way in which these 'virtual' currencies could be regulated in order to deal with financial obligations like the payment of taxes, and to avoid the use of such currency as a tax haven or to fund illicit activities. States responded in different ways to this dispruption. Some adopted a defensive approach, others a permissive innovation-first approach, and yet others a permissive but defensive approach.

The defensive approach saw some states ban the trade and investment in all types of cryptocurrencies and even criminalise its use. Thailand was the first country to ban the use of the Bitcoin in 2013 on the ground that it was not a currency. China likewise banned Bitcoin exchanges in 2013. While in 2014 Bangladesh also banned the use of Bitcoin citing potential harm arising from the absence of a centralised payment system, Russia's attempt in 2015 to pass a law banning the use of digital currencies alongside the rouble, is yet to reach the State Duma. Others like Singapore did not take any action but issued a series of warnings. Most states clamped down on Bitcoin's unregulated use, concerned that cryptocurrencies could jeopardise financial and economic policies of the state, be used as an off shore tax haven, or create unfair competition. The United States of America's Securities and Exchange Commission clampdown on Bitcoin exchanges is an often cited example. In the first criminal securities fraud case related to cryptocurrency in America, Trendon Shavers was found guilty of operating a Bitcoin-related Ponzi scheme through his Bitcoin Savings & Trust in which investors were promised a daily profit of one percent on their investments. Shavers later vanished with a large sum of Bitcoins in August 2012.[18]

This pre-2015 period was characterised by inconsistencies in policy goals arising from a lack of conceptual clarity surrounding the Bitcoin- the first cryptocurrency. In the United States for example, in 2014 the Inland Revenue Service viewed virtual currencies as a taxable property (IR Notice 2014-21; IR Notice 2014-36) whereas the United States Commodity Futures Trading Commission viewed cryptocurrency as commodity. Besides it was difficult to monitor and control how this currency is used.

Since 2015 with the expanded use of the Blockchain and growth of cryptocurrency uses (like the Initial Coin Offerings), the regulatory landscape has changed. There is greater recognition of the Blockchain as a facilitator of data management and storage via distributed ledgers, with states like Canada deciding not to regulate its use. Equally, there is now a shift in the recognition of cryptocurrencies. Japan for example, has given greater clarity to the

[18] *United States of America v Trendon Shavers* 1:15-cr-00157-LAK- decision of July 2016.

categorisation and use of cryptocurrencies. On 1st April 2017, Japan's Payment Services Act gave recognition to virtual currencies as a payment option while providing for the formal registration of cryptocurrency exchanges. Some like the United States have a patchwork of legislation passed in a Byzantine manner (state by state) with varying conceptualisations of cryptocurrency. For instance, the Vermont law House Bill 182 that was passed into law on the 4th May 2017, offers a clarification of virtual currency as a stored value that may be centralised or decentralised, and describing virtual currency dealers as authorised money transmitters. The West Virginia House Bill 2585 has updated its anti-money laundering statutes by defining cryptocurrency as a "digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, and which operate independently of a central bank." The Bill also makes it a felony crime to use cryptocurrencies for money laundering.

While countries like China try to aggressively regulate domestic cryptocurrency exchanges amid a surge in the Bitcoin price, other states have adopted a 'wait and see' approach where no action is taken to enforce formal compliance requirements and permissiveness appears to be *de facto*. This indecisiveness may arise where states are uncertain as to whether cryptocurrencies (arguably viewed as un-regulatable private property) should be regulated in the first place, or whether the state should offer a permissive regime that enables Fintech to operate in an environment that protects the investor/consumer.

The fourth approach denotes a conflation of both permissive and defensive approaches. Regulation is sometimes framed within a permissive innovation-first approach to which there are several shades ranging from less government oversight in keeping with the libertarian origins of cryptocurrency; to co-regulation where the state partners with the cryptocurrency developer to co regulate the product. The regulatory mechanism of choice is usually defensive- through a command and control top down approach that follows the technical rules on financial products and practices (rules based). These rules are usually framed around Anti Money laundering and Know Your Customer requirements. Jersey is atypical example. Jersey's Proceeds of Crime (Miscellaneous Amendments) (Jersey) Regulations 2016 brings cryptocurrency business within the scope of Anti-Money Laundering laws. Simultaneously, Jersey's Financial Services Commission has created a regulatory sandbox in which cryptocurrency exchanges (turnover of less than £150,000 per calendar year) may test exchange delivery mechanisms in a live environment but without meeting formal registration requirements.[19] Similarly, the European Union (EU) has adopted a permissive innovation- first approach that encourages the use of regulatory sandboxes. Even so, the EU intends to bring cryptocurrency operations under the Fourth EU Anti Money Laundering Directive 2015/849. The 4th Directive will be amended by the 5th AML Directive in order to prevent the use of the financial system for the purposes of money laundering or terrorist financing. [20]

[19] More information is available at https://www.jerseyfsc.org/.

[20] A report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and terrorist financing {COM(2017) 340 final) found that virtual currencies pose a significant threat to the market, a threat exacerbated by lack of common rules.

Cryptocurrency regulation in Africa

To some extent, the African regulatory landscape resembles the pre 2015 era with most African states treating cryptocurrency as a threat to the stability of the economy, with no legal status or recognition accorded to it. This quote from Dr Patrick Njoroge, the Governor of the Central Bank of Kenya summarises the situation:

> "We do not have systems capabilities and we are yet to come up with proper policies to regulate this form of currency."[21]

While acknowledging the state's limited technical capability, the Governor's statement depicts the lack of policy (and legislative) guidance regarding the status of cryptocurrencies and protection of its users in African economies. In fact, states have handled cryptocurrencies differently, with some adopting a defensive approach via clamp downs and warnings from Central Banks about the potential risks of virtual currencies. The first warning against virtual currencies came from the Federal Reserve Bank of South Africa in 2012. From 2015 to date (6th July 2017), other Central Banks like that of Kenya, of Uganda and of Nigeria have followed suit and issued Warnings.[22] The Ugandan and Nigerian warnings come against a backdrop of fears of a lack of prioritisation of ethical behaviour by promoters of some currencies like the Onecoin leading to a mis-selling of products. Then there is the worry by the Central Banks that the cryptocurrencies may lead to the creation of a Ponzi scheme and subsequent loss of investor funds. Regulators must also deal with the question of whether exchange of cryptocurrency for fiat currency falls within money remittance under the law, a question considered in *Lipisha Consortium Limited and Bitpesa Limited versus Safaricom Limited* [Petition 512 of 2015]. In this first case ever of its kind on the African continent regarding Bitcoin transactions or settlement, the High Court found that the Bitcoin represented a monetary value and any transactions in Bitcoins were money transmissions which required prior approval from the Central Bank of Kenya. These examples, show that Central Bank warnings come amidst a lack of clear policies and laws including on ethical uses, regulatory requirements, and consumer protection.

Some states combine a defensive approach that includes warnings or clampdowns, with a permissive regime that creates a conducive environment usually through the use of regulatory sandboxes in order to enable cryptocurrencies to be tested in a safe environment. The permissive regime may offer a less strict regulatory regime and lower compliance costs to start ups. South Africa and Kenya are among those states that offer a permissive-defensive regime. The permissive approach the defensive approach is evident in warnings or clampdowns, Take South Africa for example. Despite the warning issued by the Federal Reserve Bank in 2012, South Africa has adopted a permissive regime towards cryptocurrencies based on an innovation first approach. South Africa now has the highest number of cryptocurrency users in Africa. There, Bitcoin remains the main digital currency of choice for conducting a range of transactions. The Kenyan example also shows how different regulators in the same country

---

[21] Lee Mwiti, "Central Bank Governor says Kenya not ready for virtual currencies", 30th May 2016 *Standard Digital news* at http://www.standardmedia.co.ke/.

[22] Similar warnings have been issued by other African Central Banks like the Central Bank of Nigeria (12th January 2017), the Central Bank of Kenya (December 2015) and the Reserve Bank of South Africa (User Alert Monitoring of virtual currencies issued jointly with other regulators on 13th September 2014).

may adopt radically different regulatory approaches to the same product which can send mixed messages to would be start-ups and investors. While the Central Bank in Kenya issued warnings about the use of virtual currencies, the Kenyan Capital Markets Authority created a regulatory sandbox for Blockchain based innovations namely the government securities bond.[23]

Most African states have no official position, but are in a 'wait and see' mode-adopting neither a defensive nor permissive approach. However, this is likely to change over time as payment technologies become more widespread.

How should we regulate disruptive payment technologies?

The question of how to regulate disruptive payment technologies such as cryptocurrencies is an open one. One option is for regulators to partner with Fintech for example by automating customer due diligence using real time data, algorithms and analytics via social media, and/or biometrics, and to include risk management requirements like encryption. Partnership with a cryptocurrency developer or business would require acknowledgement of cryptocurrency's libertarian ethos that eschews control by centralised bodies and sovereign power. These libertarian origins can be traced to some like John P. Barlow who maintains that cyberspace is independent and should be free from any form of control or interference from the state. Applying the genesis of Barlow's argument to crypto currencies and the Blockchain, it is arguable that the trust placed in these technologies by its users supersedes the need for an intermediary or a regulator to intervene in monetary transactions, and implies the independence of the money from government's centralised control.

Some may argue drawing on Hayek's thesis that governments should not have any control over the money supply[24] bar the need to secure financial institutions[25] or to facilitate global market exchanges.[26] A country adopting this position would prefer perhaps to create their own cryptocurrency to compete with established ones in order to guarantee the security of financial institutions or to facilitate market exchanges. Central banks may respond that they need to control the amount of money circulating in the economy as it affects things like economic growth, and interest rates. Indeed, those who argue for regulation point out that the decentralised and unregulated features of cryptocurrencies could jeopardise security, economic and financial policies of states.[27] Moreover, it is nearly impossible for regulators to monitor or control how the currency is being used due to its relative anonymity. In addition,

[23] Brian Ngugi, " Virtual Cash splits Kenya regulators" *Daily Nation* 7th May 2017 available at: https://www.nation.co.ke/business/Virtual-cash-splits-Kenya-regulators/996-3910904-153vr4s/
[24] Sarah J. Hughes and Stephen T. Middlebrook, "Regulating Cryptocurrencies in the United States: Current Issues and Future Directions" *William Mitchell Law Review* (2014) 40, 813-848. Also Nikolei M. Kaplanov, "Nerdy Money: Bitcoin, the Private Digital Currency, and the Case against Its Regulation," *Loyola Consumer Law Review* (2012) 25/ 1, 111-174.
[25] Joseph E Stiglitz, *The role of the state in financial markets* (Institute of Economics, Academia Sinica, 1993).
[26] Ethan B. Kapstein, *Governing the Global Economy* (Cambridge, MA: Harvard University Press, 1994).
[27] Jared A. Kleiman, "Beyond the Silk Road: Unregulated Decentralized Virtual Currencies Continue to Endanger US National Security and Welfare" *American University National Security Law Brief* (2013) 4/1,59-78; and Peter Twomey, "Halting a Shift in the Paradigm: The Need for Bitcoin Regulation" 16 *Trinity C.L. Rev*. (2013) 67

the fact that cryptocurrency operations are not dependent on any financial intermediary could defeat any attempt at addressing off shore tax evasion.[28]

Even so, the key question for a public currency is whether cryptocurrency qualifies as currency (cash) which is a representation of money, given the lack of a universal definition of money, or a monetary law. The difficulty is that any conceptualisation of cryptocurrency as money depends on cryptocurrency's characterisation: as a medium of exchange, a private property, a digital asset or debt, or something else. This quandary of characterising cryptocurrency is reflected in these three court decisions on the Bitcoin. In C-264/14 *Skatteverket v Hedqvist*, the Court of Justice of the European Union declared that Bitcoin exchanges were exempt from Value Added Tax (VAT) under the VAT Directive. However, the decision did not directly address the question of whether Bitcoin was money. In the USA in the *State of Florida v Espinoza*[29] the court declared that under Florida's laws, Bitcoin was not money and therefore Espinoza was not guilty of illegal money transmission or of money laundering in Bitcoin. Espinoza's case is markedly different to the earlier American decision in *Shavers* where the court declared that Bitcoin is money because it can be used to purchase goods or services.[30]

The question of whether money includes a private decentralised currency like cryptocurrency is yet to be conclusively determined. Still, conceptualising money in more flexible terms as inclusive of a transferable credit, a medium for effecting payments, a stored value or some other concept, suggests that a government should not have sole control over the supply of money. This question was considered at the first Kampala Round table in 2016, where it was found that within the current legal definitions of money and monetary control, bar an amendment to the laws, the Central Bank had no control over privately issued money.

Principled versus rules based approaches to regulation

When considering whether or not to regulate cryptocurrencies, the dilemma for states is how to protect consumers' while promoting innovation and ensuring that fintech providers meet their compliance obligations. Regardless of the regulatory approach adopted, investors and consumers alike need clarity about the nature of the product that they are purchasing, the nature of rights in that product, and the avenues for redress in the event of a breach. The problem arises when the start up or business works outside of the regulation or even creates technology to by-pass regulation. One method is for the regulator to opt for a principled based approach that focuses on consumer protection principles like fairness, non-deception and non-discrimination. The other is to maintain a focus on the technical rules that largely manage risk.

An alternative is to offer consumer protection by combining both approaches applying a more robust rights based criteria to compliance requirements in order to ensure that the service protects those vulnerable individuals who are at risk of exploitation by unscrupulous businesses. The public rights here would aim to protect the individual, institution and wider society from harms posed by illegal use of disruptive technology. The rights to be protected are not always clear cut. For instance, when do investors have equity rights in a given

---

[28] Omri Y. Marian, "Are Cryptocurrencies 'Super' Tax Havens?" 112 *Michigan Law Review First Impressions* 38 (2013) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2305863## .
[29] *State of Florida v. Espinoza*, Case No. F14-2923 (Fla. 11th Cir. July 22, 2016).
[30] *SEC v. Trendon T. Shavers and Bitcoin Savings and Trust*, 2013 U.S. Dist. LEXIS 110018 (E.D. Tex. 2013).

database, or when is a security right created in a cryptocurrency unit? Obligations of businesses include liability for breach of privacy protection. Equally, legal frameworks should prevent an unjustified restriction of individual rights by the regulatory intervention. Such intervention ought to be identify user or investor rights that are limited, as well as the criteria that governs any regulatory measure. Failing that, state intervention by way of a clampdown on a product could stifle economic rights and lead to stagnation of innovative products. Take the example of the Uganda Communications Commission proposed policy of 2014 that recommends the monitoring of activities and content on social media by the Commission. On the face of it, the policy aims to protect members of the public from online harms of a criminal nature. Taken to the extreme, the policy could lead to blocking the internet- the life blood of cryptocurrencies- which could be regarded as a disproportionate restriction of rights in public law terms.

The principled based approach would do three things: prescribe rights and liabilities of all parties including rights to privacy, property, expression, association, equality, fair trial/administrative hearing and the like; legislate on sanctions for any breach of cyber security; and facilitate recompense to victims of cybersecurity breaches. Still, we need to recognise the private law issues that are implicit in the resurgence of the idea of group identity based on communitarian values ('us' v 'them', protecting the boundaries) and to appreciate that when group identity/boundaries are under threat, individual rights may be restricted for the common good.

Maintaining a principled and proportional risk-based approach to regulation could help ensure that the service protects those vulnerable individuals who are at risk of exploitation by unscrupulous businesses. Doing so requires a review of our existing policies in order to address inconsistencies in policy goals surrounding licensing, reporting requirements and the establishment of liability-whether personal or corporate, in the regulations on cryptocurrency. We also need to establish if the content of the law is still applicable to the technological product and if not, how such extension of the law may be achieved (or not). Given that the boundaries are blurred when it comes to regulating the Blockchain – as most states are loath to regulate this technology given its potential benefits, the question of whether the Blockchain ought to be exempt from regulation ought to be explored.

Key note address by Mr Stephen Mulema, Director of Financial Markets, Central Bank of Uganda

The Central Bank of Uganda attaches importance to cryptocurrency regulation. The Bank's press release of 14th February 2017 centred on what current regulations should cover in relation to currency, and where cryptocurrencies fall in that space. This implies that there is no framework under which the Bank regulates cryptocurrencies and those who get involved in these specific products run a risk of not getting adequately consumer protection. That said, there are five important discussion points on the regulation of cryptocurrency from the Central Bank's perspective.

To start with there is a need to evaluate what gaps are created by the current monetary frameworks that we use and why then we need to have the cryptocurrencies. Are there any increased risks that we are living with at the moment? What are the risks that cryptocurrencies are bringing on the table – as well as what benefits or gaps that we can close in the current

framework? This is an area that we are looking at today as stated in the concept note earlier circulated. We really ought to justify the need to make any changes in law in the future if necessary.

Secondly, monetary policy very often requires that currencies are elastic. This means that in times of distress, the Bank may increase monetary supply to respond to shocks in the economy and conversely, the Bank should be able to do the reverse if inflation shocks are expansionary. So that begs the question of how this whole currency framework comes into play. There are issues around systems-wide fraud, especially given the current environment in which we live – where there is a lot of system hacking that is going on to the detriment of users.

The other area of interest is the use of digital currency alongside fiat currency. That has the potential to fragment the economy in the likelihood that digital currency may not be readily acceptable at least as it is at the moment in the wider retail space. We have heard that one Bitcoin is worth UGX 10 million, but it is not clear how one can use the Bitcoin in the local market down the road to buy tomatoes. Users need to let us how this will work and to let the Bank know how it could get involved, because at the moment, we need to overcome legitimate concerns regarding the use of the digital and fiat currencies alongside each other.

A third area relates to the cost 'advantage' in digital currencies over fiat currencies which might be slightly exaggerated. Why is that? There are so many costs that are currently being captured in fiat currencies that are yet to be fully incorporated in digital currencies. By this we mean things to do with restrictions for example, in anti-money laundering laws. Transaction costs are currently lower because providers and users of digital currencies do not currently bear compliance costs whereas providers of other electronic payments bear costs of complying with consumer protection laws and anti-money-laundering laws. So there is yet more to consider in terms of compliance and transaction costs. Given the limited access to the internet in Uganda where these cryptocurrencies are predominantly issued and traded, a cryptocurrency if issued alongside the fiat currency could serve only to double the expenses of the currency issuance and management.

The ability of cryptocurrencies to substitute the fiat money by playing a major role in storing value, a medium of exchange and a unit of account raises important questions surrounding the attributes of money. There are three areas that cryptocurrencies would have to take up for us to classify them adequately as currency: a store of value; a medium of exchange and a unit of account. When it comes to store of value, this is dependent on the user's belief about the future supply and demand of the existing digital currencies, which is not reliable to some extent. As you are aware, some cryptocurrencies have a fixed supply and therefore they lend themselves more to commodities than perhaps to fiat currencies. A fixed supply could then lead to an increase in the cryptocurrency's volatility that could exceed what we have in fiat currencies. Volatility needs to be addressed when considering the definitions of currency given that increased volatility is likely to draw in more speculative investors, with the additional risk of increased security vulnerabilities as well as limited liquidity and uncertainties in the long term. Combined, these types of vulnerabilities can affect the viability of cryptocurrencies as a long term currency.

The fifth item- the risks to the digital currencies that was touched on earlier with regards to consumer protection. Consumer protection has to be adequately addressed. If for example, a consumer's device containing digital currency is hacked, given the fact that digital currency is supposed to be irretrievable, how is the consumer protected within those mechanisms at the moment? If a holder of a digital currency forgets their PIN or Key, how is it recovered or is the holder likely to lose their holdings or investments? This is an important risk that current fiat currencies perhaps do not have at the moment in equal magnitude. Related to the risks, are the anti-money laundering mechanisms, concerns relating to the anonymity that digital currencies provide to each party, and anonymity of the transaction in the initial issue. We all know how important privacy is at the moment. The last area under the risk of digital framework is systems failures that can arise from time to time – and they do happen to the biggest institutions. Think about the events last week with regard to the global ransomware that could affect the overall value of the holders of these cryptocurrencies, in a manner that would not affect fiat currencies.

Lastly, in relation to this, there is always need to benchmark as highlighted in the previous presentation. Where is cryptocurrency being regulated, and how is it being classified in different jurisdictions? We know that there are rulings in some countries. We know for example some of the more firm/radical countries like China banned the financial institutions from handling digital currency transactions. Russia deemed the digital currencies as an unlawful substitute for money and was planning to pass a law that should ban the digital currencies. In 2014 the European Banking Authority identified approximately seventy risks associated with digital currencies and therefore recommended a National Supervisory Authority to discourage credit institutions, money paying institutions from buying, holding and selling digital currencies.[31]

Despite the above challenges, this does not mean that cryptocurrencies do not offer any benefit. Any potential benefit comes from all central banks using their leverage in terms of broadening the creation of currencies that can adequately store value, despite the fact that whatever is created is not fiat currency. So, it is likely that the discussions such as shall take place in this second round table are likely to gain traction so that we seek a way of addressing the challenges in order to reap the benefits of what is on offer.

Cryptocurrency investment in Uganda: Mr Ivan Kintu, Cryptocurrency Evolution Ltd

Cryptocurrency is a growing business in Uganda. The coins currently in circulation (as of 6th July 2017) in Uganda are Bitcoin, Swiss coin, billion coin, hard cash and OneCoin. The ecosystem here includes the miners who participate in the creation of the coins through mining, the investors who purchase these coins and then sell them on to the public large exchanges like Bitpesa that operates in East Africa. Potential investors need to know not only which cryptocurrency and initial coin offerings are the best ones to invest in, but also to

[31] European Banking Authority Opinion on Virtual Currencies (2014) available at https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf. Also, Opinion of the European Banking Authority on the EU Commission's proposal to bring Virtual Currencies into the scope of Directive (EU) 2015/849 (4AMLD) - EBA-Op-2016-07.

understand the regulatory climate. A roundtable like this one enables all stake holders come together to educate ourselves about the way in which cryptocurrencies can benefit the economy and how cryptocurrency enthusiasts and business can work closely with the regulators and to carry on an ethical trade.

Uganda's cryptocurrency system uses multi-level marketing over the internet as well as face to face marketing based on trust in the proprietors of the business that investors will receive their investment after they have paid their money. For every transaction in base coin, a business gets 3% of that transaction. Information is shared through the peer to peer network by a series of links among the cryptocurrency community. These are real transactions – an investor or buyer is buying a coin that is worth a particular value. Potential investors or buyers who do not wish to mine the currency themselves, may visit a cryptocurrency office in Kampala, put a fifty percent (50%) down payment in fiat currency of the cryptocurrency amount and a wallet is created for the purchaser/investor. A receipt is issued and after 24 hours when the transaction has been confirmed in the purchaser's wallet, the purchaser returns to the office with their receipt and the remaining fifty percent of the money. The seller then issues a second receipt confirming that the transaction is complete and the cryptocurrency is in the buyer's wallet. Paper receipts are issued because of poor internet infrastructure which affects the speed of this internet based transaction, and is a guarantee that the transaction has been completed.

The trade in cryptocurrency is done in the ordinary way. Two weeks ago, we bought three cars and some computers using billioncoin. Next month (August) we will host an exhibition for those persons who have billioncoin or Bitcoin, to come to purchase sugar, rice, computers, even phones using cryptocurrency. This is already happening in countries such as Philippines, and Thailand, where you can pay your hotel bills using billioncoin. This is global- the value of billioncoin in Uganda is the same value in Europe, the United States or any other country. Let me tell you '*Eno business nsava nyo settaga kukwekka ku muntu yenna* ["This is a very lucrative business and there is no need for me to hide information about it from anyone"]. The wider the publicity, the more people purchase these coins, the greater the value of these coins. This is what happened to Bitcoin and it is now happening to other virtual currencies.

Since 2008/9, when Bitcoin was created, many people called it a scam and some still do. Even when the cryptocurrency business began in Uganda, everyone was calling us '*Bafere*' (conmen). At the time, each Bitcoin cost about two hundred and fifty Uganda shillings (UGX 250/-), and during the promotion, these coins were given out free of charge. Today, the landscape has changed. One Bitcoin now costs about ten million Uganda shillings (UGX10, 000,000/-) signifying an increase of over 2500% percent. Now, we host very big events at top market hotels in Uganda, where people from all walks of life including important public figures come to invest in the currency.

In fact, in Africa there are over 118 Automatic Teller Machines ATMs for Bitcoins and one can exchange the Bitcoin for fiat currency.[32] The high cost of the Bitcoin in Uganda at ten million shillings means that only a few Ugandans can afford to buy these currencies. However, the way in which the business works is that those who do not have large amounts of money can

[32] Africa's first ATM was launched in South Africa in 2014: https://www.coindesk.com/africas-first-bitcoin-atm-ready-may-launch/.

buy smaller quantities of Bitcoin called 'Change'. 'Change' is sold for lesser amounts like fifty thousand Uganda shillings (UGX 50,000/-). This 'change' also appreciates and after about three months, the investor will earn a profit. There are other coins beside Bitcoin. The more recent one began trading on 21 March 2017 costing very little money, but by the 5th July 2017, one coin was worth US $70,000. Uganda cryptocurrency businesses are looking for ways to harness this 'fire' out there. For instance, today 6th July 2017, three groups of investors are visiting several towns in Uganda like Mbarara in order to educate people about the cryptocurrency and to encourage them to invest in it.

Fintech require clarity from regulators

Cryptocurrency businesses have got their ears to the ground waiting for clarity from the Central Bank of Uganda regarding regulation of cryptocurrency businesses. The Uganda government ought to thoroughly research this technology in order to understand ways in which cryptocurrencies can boost economic growth. Many home grown cryptocurrency businesses are interested in ploughing back money into the economy rather that facilitate capital flight, and to meet their tax obligations. It is a fact that several individuals and businesses that make money by trading Bitcoins or running an exchange do not pay tax in Uganda. That untaxed money is instead invested outside the country which leaves the Ugandan economy poorer.

Of course there are problems with fraudsters and hackers. People have had their money stolen, and some have had their accounts hacked. But these problems are everywhere. Investors sign an agreement that the price of this coin should not go down – so any 'short selling' is a loss in the business. However, the lack of awareness among investors about the value of cryptocurrency and how it should be traded to make a profit meant that sometimes, cryptocurrency received free of charge or at a low cost is sold for far less. Some people who do not understand this trade end up selling the coin for far less than the ten million Uganda shillings that it is worth. This is a sort of black market, yet even though the person's account could be blocked, sometimes the administrators themselves do not know who is selling the coin on the black market.

Countries around the world are changing their attitudes towards cryptocurrency. Where once Russia and China once banned cryptocurrencies so as to protect their own fiat currency and their economy, now due to growing demand, the same countries are considering developing their own form of digital currency. For example, since January 2016 when the Peoples' Bank of China announced its plans to develop their own coin,[33] over one million Ugandans have registered interest in investing in this currency. Following the launch of the Chinese digital currency which may be sometime in 2017, there will be several Ugandans looking to trade and invest in this currency.

It is not foreseeable that the Uganda government will ban cryptocurrency in Uganda, and even it does so, it would have to take drastic measures such as switching off or blocking the internet. Even if they did switch off the internet, tech savvy investors will merely cross to Kenya, Congo or any other neighbouring country and use the internet there in order to continue to trade in

[33] Bloomberg News, "China Is Developing its Own Digital Currency", https://www.bloomberg.com/news/articles/2017-02-23/pboc-is-going-digital-as-mobile-payments-boom-transforms-economy

the currency. Investors could also take fiat currency to those neighbouring counties, convert it to cryptocurrency and continue to trade there. So, for as long as we have the internet, investors and traders will still get rich.

PANEL 2: INFORMATION TECHNOLOGY, THE JUDICIARY

National Information Technology Agency: Mr Emmanuel Mugabi and Ms Caroline Akello-Mugisha

Cryptocurrencies like the Bitcoin are gaining momentum in Uganda, and the reality is that they are here to stay. Among the youth who are more of digital natives than the older generation, there is an open approach to tech enhanced means of making money. While in a restaurant a week ago, I overhead one waiter urging another waiter to start investing in Bitcoins because he was making money from it. This shows the extent to which cryptocurrencies have pervaded our society. Whereas there is the advantage that are people are making profits from their investments, there are also some risks, especially regarding the security surrounding these exchanges.

Although there are several legitimate businesses where investors are making money, there appears to be an increase in scams which now present new threats. To the average person, it is difficult to differentiate between a legitimate business and a scam. Sadly there are several scams in operation in Kampala. So, the issues around trust and security are need to be considered more so because cryptocurrencies are one of the main modes of facilitating cybercrime. For every hack that takes place in the world, a business is started and transacted in the Dark world where digital currency is the preferred mode of payment. The relative anonymity of the Dark Web creates some sort of trust for the users given that tracing this type of currency quite challenging. The recent ransomware attacks of Wannacry and Petya in which software is created on a computer, compromises the owner's files and a ransom payment is requested (usually in Bitcoins) illustrates both the lucrative aspect of cybercrime and the loss to consumers of money and corrupted files. Another example is from South Korea, where Bithumb-a large Ethereum and Bitcoin exchange had over 30,000 files compromised. Money and data was stolen as a result of the hack.[34]

NITA-U policy considerations

NITA's policy approach towards the issue of cryptocurrency is similar to that of the Central Bank of Uganda- namely to promote innovation while managing risk. Requirements like Know Your Customer, as well as tracking of money from one point to another are important however with a decentralised system such as that for cryptocurrency, the ledger system is complicated. It is not always possible to trace how money moves from one end to another, how it is exchanged, how it is valued. With fiat money, you can easily know and trace how money moves and know your customer. Some countries have even gone ahead to create their own

[34] Robert Hackett, "One of the Biggest Ethereum and Bitcoin Exchanges Got Hacked," 5th July 2017 http://fortune.com/2017/07/05/bitcoin-ethereum-bithumb-hack/.

digital currencies; different from cryptocurrencies and controlled by a centralised ledger.[35] States are also experimenting with cryptocurrencies through partnerships between some central banks and international banks like Citibank, and Barclays.

Regarding law enforcement, this new dimension of digital currencies and the Blockchain technology has also brought about new challenges. NITA is aware of investigations into the allegations of forged identity cards under the new National Identity Registration[36], and of forged land titles[37] following the digitalisation of these systems. All these problems highlight the lack of security surrounding consumers' data which provides avenues for hackers. This government is cognisant of this problem and intends to explore new avenues to utilise disruptive technologies safely.

NITA's main purpose is to develop information technology policies to support the current regulatory environment. At present, Uganda's cyberlaws do not directly apply to cryptocurrencies. Take the example of Electronic Transactions Act 2011. The Act does not address online businesses premises for better consumer protection in the digital world, rather the law requires a physical presence of the provider which is not always the case. Likewise, the Computer Misuse Act has offences that only cover the misuse of computers and unauthorised access. Yet, not all criminal acts fall within this ambit, and tracing suspects in hacking cases is not simply a matter of saying that the 'identity is in the numbers'. Rather, clarity in the law is needed by online businesses on the parameters of non-traditional 'crimes'.

The risk of regulatory inefficiency may arise because there are several regulators in this area of cryptocurrency like the Central Bank of Uganda, the Uganda Communications Commission and the NITA. The question of who should regulate what, is not yet resolved. Although it has been suggested by participants that all these regulators should work together, it is not clear how this arrangement would work given that the Central Bank would want to regulate the financial aspect of cryptocurrency; the Uganda Communication Commission would want to regulate the communication aspect; and NITA, the information technology aspect.

Regarding information technology infrastructure, the national uptake is varied. While in some villages in Uganda, people have and use the messaging platform WhatsApp, some people in the capital city of Kampala did not have this service. Despite this increase in the use of information technology, NITA are concerned about consumer protection, specifically who is accountable if cryptocurrency or data is stolen. This is more so because it is difficult to trace

[35] Plans by a Senegalese bank- Banque Régionale de Marchés (BRM) to introduce a centrally administered digital currency called the e-CFA have not come to fruition (http://africanbusinessmagazine.com/african-banker/senegal-creates-digital-currency-history/). The Central Bank of West African States objected to the introduction of the eCFA on the grounds that the Central Bank was not involved in the project, and warned the BRM against the use of the term eCFA to prevent any kind of confusion with the legal currency CFA that is already in use in West Africa. Malick Ciss, "West African Digital-Currency Project shunned by Central Bank" (7th April 2017) at http://sweetcrudereports.com/2017/04/07/west-african-digital-currency-project-shunned-by-central-bank/.

[36] Press Release by Uganda National Identity Registration Authority (NIRA), "Clarification on Issues Raised in the Story "Panic as National ID Data Is Stolen" (reported in the *Sunday Vision* 25th June 2017) http://www.nira.go.ug/wp-content/uploads/Publish/Press%20Release.pdf.

[37] A Commission of Inquiry on Land Matters in Uganda headed by Justice of Appeal Catherine Bamugemereire was began its work into the policies and processes of the acquisition, administration, management and the registration of land in Uganda in May 2017.

the culprit. The Central Bank and the commercial banks operate a system that offers redress and oversight in the event that a bank collapses. This means that the consumer could recover their money. However, it is not clear to whom aggrieved consumers should turn if a cryptocurrency business collapses and an investor loses their cryptocurrencies.

Going forward, NITA recognises that technology develops over time and in this context, we are planning to do a gap analysis of the laws and policies to see what needs to be changed. The analysis will be done through a stakeholders' engagement. Much as it is desirable for the economy to develop through the use of electronic platforms, NITA prioritises public awareness and public protection. Regarding the latter, NITA has measures to enhance public protection. For example, with the framework of the Electronic Signatures Act, NITA is looking to put in place a Public Key Infrastructure (PKI) comprising policies and the infrastructure that develops electronic certificates or digital certificates similar to those digital signatures and certificates in use by the banks. NITA hopes that the PKI will offer some level of protection, but given the unique attributes of cryptocurrency, we need to resolve policy challenges that the technology brings.

Judicial Training Institute: Dr. Gladys Nakibuule-Kisekka, Deputy Director Law Reporting and Research and Training

The Judicial Training Institute (JTI) has the mandate is to track the gaps in the judicial adjudication practices, and to offer through research, juridical solutions to dilemmas in law. In adjudicating cases on cryptocurrency conflicts are bound to arise and the courts need to be able to resolve those conflicts within legal frameworks and to order legal redress. The Commercial Court for example, has handled cases that touch on the regulation of electronic money- the precursor to cryptocurrencies.[38] Then there is the case of *Guster Nsubuga and others* who were found guilty by the Anti-Corruption Court of offences under the Computer Misuse Act including unauthorised use and interception of computer services, unauthorised access to data, and electronic fraud all resulting in the loss of over two billion, four hundred million Uganda shillings.[39] In modern times, faced with a case involving cryptocurrency or the Blockchain, the lack of legislative and regulatory guidance in this area may leave judges, magistrates and other judicial officials in the 'dark' about how disruptive technologies are regulated by law and policy, and the intended and unintended consequences of the regulation.

The role of judges in the interpretation of and application of law and policy is relevant because although judges in Uganda may not make law, they certainly influence the development of the law through their judgements. Take the example of constitutional interpretation under article 257 of the Uganda Constitution, where judges need to determine whether a right has been infringed, has been violated, or is in conflict with another right. Functional equivalence in

[38] Examples include the case between MTN a multinational telecom company and Ezee Money where the defendant's services were terminated by MTN for not meeting the eligibility requirements for operating as a cash transfer service. In *Ezee Money (U) Limited V MTN Uganda Limited* Civil Suit No. 330 of 2013, the High Court held that MTN's actions amounted to unfair competition in the communications sector.

[39] *Uganda versus Guster Nsubuga, Farouk Mugere Ngobi, Owora Patrick and Byamukama Robinhood* HCT-00-AC-SC-0084-2012.

legislation may create a challenge in adjudication if the case is about the determination for example of rights in cryptocurrencies.

The judiciary needs to be part of this conversation in order to make a meaningful contribution to jurisprudence- one that deals with the complex questions addressed above. This contribution ought to address addressing the knowledge gap about the process and content of cryptocurrency and the Blockchain that is problematic to consumers, regulators and tech companies alike. Addressing this gap needs skills training including creating awareness about principled approaches to regulating cryptocurrency and capacity building. Then there is the question of the supply of equipment to enable judicial officials especially at the lower level of Magistrates, to use computers to process the court recordings rather than doing this in long hand. Accessing computers at work can also help one to better appreciate the complexity of internet based activities like cryptocurrency.

Recommendation

A starting point is for all stakeholders including Fintech start-ups, businesses, policy makers, regulators and legislators to work with the judiciary in order to create cross institutional dialogue that engages with the whole system. For while the judiciary together with other agencies like the Police and the Uganda Law Reform Commission are part of the sector-wide Justice Law and Order Sector (JLOS), most of the financial regulators including those here present like the Central Bank of Uganda, Uganda Communications Commission, and National Information Technology Agency (NITA) are not part of JLOS. This means that crucial discussions on cryptocurrency and the Blockchain regulation could exclude the judiciary, yet judicial officials are a pivotal part of the dialogue on how to adjudicate in such cases. What is needed is for all stakeholders to agree on a strategy and an entry point.

PLENARY SESSION 1

Cryptocurrency inflationary tendencies

Concerns were raised that the current trends of hoarding rather than spending cryptocurrencies could lead to their inflation or even deflation. Treating cryptocurrency as a unit of account or medium of exchange meant that it could circulate in the economy. However, with about 85% of Bitcoin currently hoarded, and only 15% in circulation, cryptocurrencies were still treated as investments not as a unit of account or a medium of exchange. Onelife Uganda that sells Onecoin[40] is but one example of a business that encourages people to invest in the cryptocurrency and to encourage hoarding which could ultimately lead to deflation.

Taxation - use of current laws to prevent tax evasion

Crypto currencies are treated as a speculative digital investment or asset by most Ugandans. Even so, at some point the asset holder may have to exchange the cryptocurrency for fiat currency if only to pay taxes.[41] In the Ugandan colonial era, the introduction of taxes forced

[40] https://onecoinuganda.wordpress.com/.
[41] Adrian Blundell-Wignall, "The Bitcoin Question: Currency versus Trust-less Transfer Technology", (2014) OECD Working Papers on Finance, Insurance and Private Pensions, No. 37, OECD Publishing. http://dx.doi.org/10.1787/5jz2pwjd9t20-e

people to get some form of currency – be it cowrie shells or coins, in order to pay that tax. In today's setting, if a community decided to adopt a cryptocurrency; for as long as the state still demands tax in Uganda shillings, the cryptocurrency holder will have to convert it to fiat currency which could act as a limitation on how much cryptocurrency can be hoarded.

Uganda's Income Tax Act [42] provides for a capital gains tax on the disposal of an asset, but the lack of guidance regarding whether cryptocurrency is a property whose disposal attracts payment of a capital gains tax has made it difficult for the Uganda Revenue Authority to know which rules to apply when determining the cost of the cryptocurrency before taxation. This is more so if an investor or trader has accumulated value from the time of purchase of the cryptocurrency, but is dishonest and does not declare the actual amount of profit made. In such a situation, an investor could end up paying much lower capital gains tax on that difference. This is more so where the transactions took place between private individuals who, unlike formal exchanges, may not have used a fixed rate of currency exchange.

In addition, cryptocurrency transactions are difficult to trace owing to their largely anonymous nature quite unlike credit card transactions that are easy to trace. In 2012, in the *Uganda vs Guster Nsubuga* case where the URA motor vehicle database was hacked, the evidence used against the offenders included credit card transactions that showed which credit card was used to purchase the hacking software.

Participants recommended that the tax body (URA) use Section 16 (2)(d) of the Value Added Tax Act that deals with the taxation of electronic services given the general trend for tax bodies to consider that if a good or service is bought on line, it is treated as liable to VAT. Equally, URA could treat cryptocurrencies as a commodity that is liable to attract VAT tax. While participants noted the difficulty faced by the URA in tracking online transactions, it was noted that URA had begun research on ways to tax online/e-commerce services, and to overcome the challenges of anonymity in the tracing of tax evaders outside of Uganda's borders.

Protecting the Public interest

Participants discussed which public authority was best placed to protect public interest in cryptocurrency investment schemes – law enforcement agencies like the Police or the Directorate of Public Prosecutions, the courts, or the Central Bank? The Bank of Uganda's mandate under Article 162 (1) (b) of the Constitution is to "regulate the currency system in the interest of the economic progress of Uganda" although the scope of this interest is not defined. Courts have also defined public interest to mean that the public has "confidence that court will enforce the law to uphold the "sanctity of business efficacy in a free market economy". [43] Participants questioned whether such financial and associated regulators of cryptocurrencies ought to have guidelines regarding protection of the public interest.

It was agreed that there was need to define public interest in a manner that takes into account the different conceptualisations of public interest in the constitution, in existing laws, court

[42] Income Tax Act Cap 340 (Part VI - Gains and Losses on Disposal of Assets) on gains and losses on disposal of assets (s.50); Disposals (s.51); Cost base (s.52); Special rules for consideration received (s.53); and Non-recognition of gain or loss (s.54).
[43] *Ssebaduka v Warid Telecom Limited* (Miscellaneous Application No. 204 of 2014, Decision of 20 August 2014.

cases and regulations. Such definitions ought to be aligned with consumer protection requirements like Know Your Customer with the right sort of compliance mechanism in place.

PANEL 3: POLICING, COMMUNCATIONS, AND INTELLIGENCE MONITORING

Policing Cryptocurrency fraud: Mr Dan Munanura, Assistant Commissioner of Police and Director, Electronic and Counter Measures, Uganda Police Force

To date, the electronic counter measures department has not registered any complaint due to the lack of a law proscribing acts related to cryptocurrency fraud or cybercrime. The Police know that people are using cryptocurrencies and that the Bank of Uganda has not advised people not to trade or invest in them. By contrast, the police record many complaints that relate to the regulated businesses that offer mobile money services. For example, in months of August and November 2014, mobile money fraud caused a loss of over 207 million Uganda shillings (approximately $ 80,000 United States dollars) to consumers. In 2014, Automatic Teller Machine (ATM) fraud led to a loss of over 1.2 billion Uganda shillings (approximately $ 460,000 United States Dollars)[44]. Fraud in mobile money has also been exacerbated by the non-registration of sim cards by the Uganda Communications Commission. During investigation of cases of fraud, it has been established that not all the sim cards are registered, making it difficult to trace the owner of the mobile phone used in the commission of the fraud.

Regarding cryptocurrencies, the police have engaged online with the registered cryptocurrency agents in Kampala and have established that sellers of the Bitcoin prefer to transact in fiat currency sent via mobile money platforms. The Bitcoin sellers want payment upfront and are not willing to meet the buyer in person. Police investigations also indicate that local cryptocurrency agents are also agents for much bigger exchanges some of which are located outside Uganda. Usually, fraud occurs because the potential buyer has trust in the online agent that they are dealing with, but when the seller fleeces the buyer and the case is reported to the police, it is difficult to investigate for several reasons.

The lack of sector specific laws makes it difficult for the police to apprehend cybercriminals and those who prey on unsuspecting consumers. A recent example illustrates this problem. In July 2017, a company called Cryptosave held an assembly in Mubende to talk to local residents about making investments in OneCoin. Residents were advised to buy OneCoin on the promise that it would appreciate with time and the proceeds could be invested for the benefit of their children and grandchildren. When a complaint was reported to the police, the only charges that the police could bring against the suspects were that of 'Holding an unlawful assembly' under Section 118 of the Penal Code as the suspects claimed to be operating businesses that were legally registered. In Kasule Lusuula, Dr. Saturday and others (Police case Mubende CRB 843/2017), the suspects gave intelligence that helped the police find the offices of OneCoin in order to verify those behind its operations for which the Central Bank

[44] Cybercrime Barometer, A Uganda Police Centenary plus Awareness Campaign Paper available at http://www.upf.go.ug/cyber-barometer/.

issued a Public Warning (February 2017). The police sought further clarification regarding the registration of the business, but in the meantime, the charges of an unlawful assembly stood.

Ordinarily in such cases, the police ought to get a court order to search the physical premises for the equipment that was used to defraud the innocent consumer. However, given the intangible nature of this online trade, such a court order would be framed in vague terms as it is difficult to identify the digital identity and location of the seller. In this context, anonymity is a big challenge for the police investigator. Furthermore, the absence of clear regulation leads to jurisdictional challenges arising from the cross border nature of cryptocurrency. So, even if cryptocurrency were banned in Uganda, traders can continue to use cryptocurrencies in more accommodating regimes elsewhere in the world.

Recommendation

Arguably, the current laws like the Computer Misuse Act, the Electronic Signatures Act and the Electronic Transactions Act could be applied to instances of fraud caused by hacking. However, what is needed is a clear definition of cybercrime arising from the misuse of disruptive technology- one that deals with the issue of anonymity. The Central Bank of Uganda as a regulator are doing their part to protect the public interest, but we need a multi-sectoral approach to give clarity on (among other things) the definition of, and liability arising from the misuse of cryptocurrencies. This unified approach would be vital particularly where other actors like prosecutors or judges may also have limited knowledge about the nature of cryptocurrency fraud, on the application of law in those circumstances, and what sort of redress to offer the aggrieved party. Any regulation should address these issues.

Uganda Communications Commission: Mr Julius Mboizi, Senior Officer, Legal Affairs

As a regulator in the Communication sector, the Uganda Communications Commission (UCC) like all regulators, looks to balance the risks to consumers from cybersecurity fraud particularly data protection, with facilitating and encouraging innovation in the wider context of fintech such as in cryptocurrency and the Blockchain. Regulators would not want to stifle an innovative product that aids development, and so the regulatory approach matters. Thinking back to the emergence of mobile money, the Central Bank's 'Wait and See" or "Hands off' approach at the time (pre 2013) was one of the reasons behind the success of mobile money use in Uganda.[45] The same attitude by the regulators in Kenya led to the widespread use of mobile money there. By contrast, South Africa adopted a more restrictive approach towards mobile money, which is one of the reasons why there has not been a widespread adoption or growth of mobile money in its market.

The extent of the regulation is equally important. Firstly, there is the extent of compliance as the more traditional financial institutions have to comply with a wider range of laws and regulation, while the start-ups in the wider fintech space that are providing similar services,

[45] For an early study on the adoption of mobile money in Uganda see Ali Ndiwalana, Olga Morawczynski, and Oliver Popov, "Mobile Money Uganda: A Preliminary study" (2012) available at SMA. http://www.gsma.com/mobilefordevelopment/wpcontent/uploads/2012/06/m4dmobilemoney.pdf

are not subject to the same level of scrutiny or compliance requirements. So regulatory 'arbitrage' – where start-ups may use loopholes to avoid regulation, is a concern for the UCC as a regulator. Secondly, there is the challenge of inadequate inter-operability of systems. Currently, the UCC under a Memorandum of Understanding with the Central Bank of Uganda is looking at the inter-operability of mobile money systems with telecoms in order to improve the way in which the different systems exchange and use consumer information (data).

Recommendations

The UCC regulatory and policy recommendations can be summed up as follows. Firstly, there is need to adopt a more principles-based approach to regulation rather that strictly compliance-based in order to discourage 'knee jerk' reaction to problems that may arise in this fintech area. Secondly, there is need to adopt a technologically neutral approach to regulation. So rather than focus on the particular fintech, it would be better to look at the services that they provide, to consider how those financial or banking services are provided, and to find out what needs to be addressed in order to improve consumer protection. This approach could help increase scrutiny by regulators and prevent unfair competition

In order to strike an appropriate balance between regulating for risk and promoting innovation, several countries have adopted a regulatory sand-box approach. There, if a new product comes up where there is no existing regulation, the start-up is allowed to operate in the space and is sometimes subjected to looser compliance requirements than the more established traditional players. The idea is to encourage this new product in a limited and monitored environment, so as to protect the wider system and consumers. Such oversight continues until such a point where the regulators have a better understanding of the product including whether it can deliver strong returns and spur growth in the economy. The regulator will either develop appropriate regulation for the product, or to bar it from entering the wider mainstream market. A good example is the launch of the M-Akiba Bond by the Kenya Capital Market Authority. All these policy objectives are underpinned by the need for more inter-agency cooperation and harmonisation of regulation.

Notably, one of the unregulated spaces that requires urgent action is in relation to offering redress to complaints. If something goes wrong to a consumer transaction, there is need for some sort of regulation to provide redress. All these proposals will require further clarity.

Financial Intelligence Agency (FIA-Uganda): Ms Esther Kagira-Aikiriza, Manager, International Relations and Strategic Analysis

The Financial Intelligence Authority is a new agency established on 1st July 2014 under Section 18 of the Anti-Money Laundering Act (AMLA), 2013, in order to coordinate the implementation of the country's Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) regime. Simply put, money laundering is the act of obscuring the true origin of illicit funds and making them appear legitimate. The money laundering cycle is in three stages of 'placement' where proceeds of the crime are introduced into the financial system to relieve a criminal of their "dirty" assets; 'layering', where the illicit funds are separated from their source to conceal their origin; and 'integration' where the illicit funds are

returned to the criminal for their use. Terrorist Financing (TF) covers the acts of soliciting, collecting or providing funds, from both licit and illicit sources, with the intention of supporting terrorist activities or organisations.

The ease with which money and valuables can now move across borders means that regulatory authorities must be able to address emerging risks like transnational crimes that are facilitated with new technologies like cryptocurrencies. The cryptocurrency business brings with it certain features that facilitate its use for money laundering and (sometimes) terrorism financing. Fast transaction times, low transaction costs, lack of a centralised authority, trustworthiness in payment and cryptographic security are just some of these features.

The potential risks arising from cryptocurrency use in Uganda are three fold. Firstly, the lack of awareness about cryptocurrencies means that they are too sophisticated for the ordinary Ugandan, the majority of whom are not digitally literate. The technology requires a certain degree of understanding before it can be employed by users, regulators and law enforcement agencies. The second risk arises from the fact that it is not easily traceable. Anonymity can be a double edged sword because it is good for innovative business, but it could also be used by criminals who launder money and purchase illegal items on the internet without the risk of being traced. Thirdly, given its global cross border reach, the responsibility for AML/CFT compliance, supervision and/or enforcement can become blurred when dealing with different national regimes.

FIA AML/CFT policy developments

In line with the Financial Action Task Force Recommendations (2012)[46] specifically Recommendation One which advises countries to carry out national risk assessment and apply a risk-based approach, Uganda has just concluded its risk assessment. The final report is not yet ready as the draft is still under consideration at the Ministerial level. Nonetheless, at the moment cryptocurrency is not a risk as far as money laundering financial transactions are concerned, mainly because Uganda runs a largely informal economy where cash is kept sometimes under mattresses, and land is purchased with cash and without going through the banks or lawyers. Uganda has also registered successes in prosecuting money laundering.[47]

Recommendations

Despite the lack of consensus as to whether cryptocurrency should be subjected to some form of regulation by a government authority, there is need to consider guidance developed by bodies like FATF that are aimed at helping public authorities and the private sector to identify and to effectively address money laundering and terrorism financing risks associated with virtual currencies. Uganda, ought to regulate this nascent area particularly at the time of exchange from the virtual to the fiat currency.

---

[46] Financial Action Task Force International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (2012).Also the updated version of October 2016.

[47] Successful prosecutions for money laundering offences include *Uganda v Sserwamba David Musoke and 6 others* (HCT-00-AC-SC -0011-2015) Decision of 30th May 2017.

Several things could be done. The first is for regulators to amend their laws to provide an avenue to regulate virtual currencies. Such laws should provide a definition of virtual currencies alongside the requirements for disclosure of key online information in order to support the Know your Customer (KYC) due diligence requirement. Secondly, cryptocurrency exchanges and related businesses should provide for or maintain a security bond with their regulators. This proposed requirement for the bond guarantees some sort of security to recompense a person who is defrauded by the business, and ought to be specified in a law. These measures should go hand in hand with public awareness regarding virtual currencies schemes for both the public and for the different stakeholders including law enforcement agencies. Finally, skills training and capacity building is necessary if law enforcement agencies are to effectively investigate cybercrimes; to apprehend culprits; and to follow the illegal money. It is anticipated that any proposed regulations will offer clarity to all stakeholders as well as offer protection to law enforcement agencies.

PLENARY SESSION 2

Challenges to fiat currency

Three possible challenges to fiat currency could arise. The adoption of cryptocurrencies could in the future, pose a significant challenge to the Central Banks' ability to influence the price of credit in the whole economy. As the use of cryptocurrencies becomes widespread, there was a possibility of loss of consumer confidence in the fiat currencies. Moreover, the widespread use of cryptocurrencies could make it more difficult for statistical agencies to gather data on economic activity which data is used by the government to shape fiscal and related policies. Virtual currencies could also challenge the Central Bank's control over the important functions of monetary policy and exchange policy.

Developing an institutional arrangement around the peer to peer networks

The need to explore ownership of a regulatory framework framed around the peer-to-peer framework was underscored. It was appreciated that there was need for some level of control, and for a deeper understanding of the risks of having an arrangement which ensures that payments technology are safe, efficient and transfer value in a speedy way. Still, there was no need to abandon manual or paper based instruments –given the difficulties of establishing the key actors in this fintech space; coordinating the oversight process; and understanding the risks of putting any regulation in place.

The first step was to create public awareness in order to enable regulators understand how such an arrangement works, consider any benefits and risks of such an arrangement, and look at possible ways of evaluating the arrangement in order to improve it. Next, was for regulators to work with the fintech partners to discuss how this arrangement could be regulated given that there were various actors and regulators. Most importantly, in order to protect consumers from hackers and unscrupulous and unethical behaviour, there was need for clear guidance about how this arrangement could be co-ordinated, including the place for a central authority if required.

Legitimisation of cryptocurrency

The importance of legitimatisation of the cryptocurrency trade was viewed as one possible way to widen financial inclusion and to protect consumers from fraud and unethical behaviour. Regulation could help the established and already registered business gain legitimacy and trust from consumers and regulators. However, it was noted that even with over 1,189 Bitcoin ATMs worldwide, cryptocurrency had not yet been accepted as a medium of exchange at the national level in many states. What was needed was a roadmap that drew on knowledge of the key players in the cryptocurrency environment like developers, miners, investment schemes, and exchanges on how the regulation could be developed; what alternative agreements might exist other than trust in the cryptocurrency; and what would back up such agreements.

Privacy – an ethical dilemma

Participants appreciated the difficulty in trying to regulate a cryptocurrency that is underpinned by the private networks, but pondered whether the concept of privacy is dead given that every detail on the public distributed leger can be viewed by those participating in that cryptocurrency. The ethical dilemma is that if people have given up their privacy in the course of using the wallets or other services, it was questionable what role the regulator could play in protecting that privacy; to what extent that protection could be achieved; and whether consumers should merely accept a certain level of loss of privacy and the harms that may come from that- like fraud, hacking and the like.

Encryption was viewed as a possible regulatory tool despite the fact that not all encryption is fool proof and could be decrypted. It was recommended that regulators should consider how encryption and other tech enabled protections could be drawn upon to offer effective consumer protection.

Cultivating a collaborative co- regulatory approach

Participants called on the public sector including policy makers, regulators and legislators to develop an open positive attitude towards Fintech, given the willingness of those in the cryptocurrency sectors like developers, miners, investors, exchanges to work with the government. It was acknowledged that several companies working in this area were too intimidated to attend such Round Tables, yet the cryptocurrency market covers over one hundred and twelve (112) districts in Uganda- much more than the branches of the Central Bank. Such large coverage meant that a collaborative co- regulatory approach might offer better opportunities for both sides to reap the benefits of fintech; avoid regulatory arbitrage and over regulation; and propel Uganda towards the middle income country that it aspires to be.

Managing Risk

The risk in any business like losses of money was widely acknowledged. There was the fear of the cryptocurrency being some sort of pyramid scheme in which consumers at the bottom lose out when a business folds and cannot be traced. The lack of physical evidence of the transaction, the lack of collateral, coupled with the indication that purchases of these coins

and investment in Initial Coin Offering may be based on speculation are well known risks. Managing these risks meant putting in place a system that identified key players (merchants, users and the like), identified what should be regulated and what systems for recompense were needed. Regulation had to be based on understanding the product very well. If the Central Bank or any other regulator were to regulate this sector, it would give confidence to Ugandans that this the product or service was worth using and investing in. Where risks affected the consumer, the regulator would have to help the consumer.

Participants agreed that the FIA suggestion of having a bond as security could help investors who were ripped off by unscrupulous businesses to recover their monies. For established businesses, part of the licensing requirement could include a bond of about 50 billion Uganda shillings as a form of insurance taken out by the service provider.

PANEL 4: SOCIO CULTURAL LEGITIMACY OF REGULATION

Drafting socially relevant cryptocurrency regulation: Dr. Anthony Kakooza, Dean of the Faculty of Law, Uganda Christian University, Mukono (UCU)

The phrase: *'Government ettuyambe'* [Government should help us] is apt for this panel discussion. At one level, this statement means that whenever people are in trouble, they run to the government for help. Yet at a secondary level, this phrase could mean that consumers or investors expect the government to have some sort of regulation to deal with problems that may arise in their day-to-day transactions. Therefore, it appears that we need to accept that for good or bad, there is need for some form of regulation of cryptocurrencies - be it defensive protection or positive protection. One extreme method is to declare cryptocurrency illegal in a country. The other method is to regulate its use in such a way that it follows certain parameters. At the very least there needs to be some guidance to investors and consumers. To date there is no 'best practice' as such in any region globally,[48] but we could explore developments from some countries that have gone ahead to regulate cryptocurrencies, to see the trends.

Japan is in the lead with two specific pieces of legislation. Both the Payments Services Act and the Act on Prevention of Transfer of Criminal Proceeds amended in 2017, bring virtual/digital currency exchanges within the context of payment and money laundering regulations. Denmark has gone as far as to reduce cash-based economy and rely instead on digital currencies. United Kingdom considers cryptocurrency as private money which in this case is not subject to VAT in a peer to peer setting where both persons are trading in cryptocurrency unless the transaction requires cryptocurrency to be converted into foreign currency or to buy goods, in which case any gains made will be taxed. Finland exempts financial services from VAT for digital currencies or cryptocurrencies. Although Australia removed the 'double tax' on Bitcoins and other cryptocurrency users, Australia is focused on the 'Know Your Customer' system to ensure that transactions are clean. In the United States

[48] See generally Primavera de Filippi, "Bitcoin: a regulatory nightmare to a libertarian dream", *Internet Policy Review*, 3(2); and Ed Howden, "The Crypto-Currency Conundrum: Regulating an Uncertain Future" *Emory International Law Review* (2015) Vol. 29, 741-798.

of America as stated earlier, the regulation is controlled at the federal state level. Some states are giving cryptocurrency immediate recognition, yet others are still wary about it. Initially, the Financial Crimes Enforcement Network (FinCen) considered virtual currencies as money services business and not a currency. But since 2013, cryptocurrencies are viewed as convertible decentralised virtual currencies, so they are gradually getting recognition state by state. Canada's regulation is in the nature of anti-money laundering and counter terrorism laws. Germany's Federal Financial Supervisory Authority recognises cryptocurrencies as legally binding financial instruments, under a category called units of accounts.

Some countries have regulation that is more protective. Iceland for example want to protect the Icelandic fiat currency and in so doing, digital currencies cannot be traded under their Foreign Exchange Act. Vietnam consider virtual currencies illegal and view them as an avenue for criminal activities. In China, individuals may deal in cryptocurrencies, but government institutions are not allowed to deal in cryptocurrencies. Bolivia, Kazakhstan and Ecuador have not granted any legal recognition to cryptocurrencies. They are seen as illegal.

Notably, there are no real precedents as such, because each nation has tailored its internal system to suit their country's socio- economic and political needs. Uganda needs to do the same in order to see what works given that Uganda is an agro-based economy. The majority of the Ugandans are not tech-savvy yet cryptocurrencies are more suited to those who are knowledgeable about this payment technology. In considering regulation in Uganda, we need to ask ourselves if we should follow the approach of countries that have banned or limited the use of cryptocurrencies, or to be more permissive. Regulators need to take into account the fact that cryptocurrencies have to compete among themselves through the creation of substitutes that can gain market advantage through lower entry points like the free coins given away in Uganda. For instance, Onecoin competes with the Bitcoin. How this affects the potential consumers is unknown and needs further investigation.

Recommendations

Regarding a technologically neutral regulation, the question is how far a regulation can be tech-neutral if at the drafting stage, one cannot speculate on the parameters of the future technology five years down the road? These are some of the challenges faced by legislative drafters such as those at the Uganda Law Reform Commission. At the time of drafting the Uganda's cyberlaws one of the concerns was how to draft technologically neutral regulation that would not be rendered irrelevant when it is passed as law, but the technology has evolved.

The regulators ought to work collaboratively with legislative drafters and those in the cryptocurrency business to see how regulation can be drafted. Such regulation, ought to target the service, rather than target the service provider. By regulating the service, the regulator could better control how the service provider works.

Legal challenges to regulating cryptocurrency: Dr Ronald Kakungulu-Mayambala, Senior Lecturer, Makerere University School of Law, Kampala

Let us consider the five legal challenges that arise in the regulation of cryptocurrency. The first challenge is how to increase the adoption of cryptocurrencies in Uganda by getting the public to use cryptocurrencies in their day-to-day transactions. Right now, the dominance of cash is

such that some supermarkets in Uganda are hesitant to accept debit cards and credit cards-they prefer cash. With this low penetration of electronic money, it will take a while for cryptocurrencies to be appreciated as a mode of payment or exchange despite the fact that cryptocurrencies offer instantaneous real time completion of transactions. Increasing the adoption rate means getting a shift in people's thinking towards an alternative to fiat currency and its underlying technology.

The second challenge is how to adapt the legal framework to accommodate disruptive technologies. Before coming up with policies to regulate cryptocurrencies, the regulators need to investigate whether they can use existing laws and would need to choose carefully from the myriad of laws. Alternatively, regulators could work simultaneously with several sets of laws. Despite the existence of the cyberlaws[49], regulators need to investigate the area of consumer protection, because Uganda has a draft Consumer Protection Bill 2004 but lacks a specific law on consumer protection.[50] Even though Uganda's cyberlaws have provisions that deal with consumer protection, these sections do not offer adequate protection from rogue traders. The criminal laws also need to be revised so as to find a place for acts like counterfeiting contained in the draft Anti-Counterfeiting Bill 2015.

The other important aspect is the law of banking, specifically e-banking. E-banking is an area of concern with regards how to prevent terrorism financing. The state is very concerned about which money is exchanging hands with whom, and when these transactions are taking place. Cryptocurrency regulation therefore needs to be streamlined with the legal framework on banking and anti-money-laundering in order to better prevent terrorism financing.

The question of data protection and protection of the privacy of the users remains of great significance. The media has stressed how data protection is very important in this era of rampant misuse of information, but this is an area which is not well understood at all. Issues of data protection and privacy in Uganda are not taken seriously. For instance, how did the National Identification Registration Agency (NIRA) ensure that personal and sensitive data is protected in the process of sharing this data with the telecommunications Big Six[51] under the NIRA-UCC arrangement? Such aspects are covered in the Clauses 27 and 28 of the Data Protection Bill, but since 2004, this bill is yet to be passed by Parliament.[52]

Assuming that cryptocurrencies through companies like Bitpesa penetrate the Ugandan market in a big way, the fifth challenge that will arise is the need for a competition law and policy – what the Americans call anti-trust. Such a policy and law would prevent unfair trade practices in the market. Again, this is a green area where we have the National Competition and Consumer Protection Policy (2014) which has been in place for some time now and the draft Competition Bill 2004 that is yet to be passed by Parliament. Therefore, everything that

[49] The Computer Misuse Act 2011, the Electronic Transfer Act 2011, and the Electronic Signatures Act 2011.
[50] Explicit guidance for the banking sector can be found in the Bank of Uganda Financial Consumer Protection Guidelines, 2011. Other consumer related protection laws are the Financial Institutions Act No. 2 of 2004 and the Micro Finance Deposit-Taking Institutions Act No. 5 of 2003.
[51] The big six telecoms are MTN Uganda, Airtel Uganda, Uganda Telecom, Africell Uganda, Smile Telecom and Vodafone Uganda.
[52] Ronald Kakungulu Mayambala, 'A Critical Review of Uganda's Data Protection and Privacy bill 2015 Opportunities and Threats to Citizens' (September 2016) ,4 http://ugandajournalistsresourcecentre.com/critical-review-ugandas-data-protection-privacy-bill-2015/

needs to be done requires a robust legal framework that can help resolve among other things any dispute that may arise and offer recompense.

Recommendation

Given the limited appreciation of commercial laws, especially in the area of information communication technology among Ugandans, the onus is on the state to provide nation-wide awareness raising programmes and sensitisation on how laws would work to build security and trust among the public in cryptocurrencies.

Socio-cultural transformation' of regulation: Dr Maureen Mapp, Birmingham Law School, University of Birmingham

Rural based groups continue to adapt to modern technology and to use mobile phones to get mobile (electronic) money (GSMA report 2016 on mobile money) despite being largely unbanked and excluded from low cost financially inclusive payments systems. In Africa, Bitpesa is predicted to lead this transition and to enable cryptocurrency to penetrate East Africa[53] just as it has done elsewhere like in Ghana (Beam), Nigeria (Bitstake), and Zimbabwe (Beat finance). Some like Garrick Hileman might disagree, reasoning that even if a higher adoption rate for cryptocurrency is achieved in developing nations, cryptocurrency will develop but only among those who have got bank accounts or are certainly highly educated, not the unbanked.[54] Taking Hilleman's concerns on board, the potential for rural Africa to leapfrog onto the cryptocurrency business via mobile money raises important questions about legitimising regulation in a manner that accommodates norms and practices of non-state societies.

Socio-cultural legitimacy is an important part of the 'cultural transformation' of regulation given the resurgence of national identity that is framed around communitarian values, localised norms of justice and processes. Predictably, people who are vulnerable due to age (like older non-tech savvy people), education (semi-literate or illiterate), gender (mainly women), or have some form of impairment including learning disabilities, may be targeted by unscrupulous cryptocurrency businesses and exploited. Such vulnerable people may not want to involve the formal avenues for redress like the police, the courts or other organs of the state but may instead prefer to use their own customary systems or local council courts as a first stop for dispute resolution. This may be because these fora are more readily accessible in terms of language, distance and the application of familiar norms and values. Indeed, there is anecdotal evidence of the preference for localised justice in the Justice Law and Order Criminal Justice Baseline Survey of 2002. The survey established that public confidence in national law courts was waning and people resorted to kinship systems, including clan courts, to get atonement for victims through compensation. [55]

The societal set up of traditional systems such as the Kingdoms of Buganda, Bunyoro or Toro, of Chiefdoms like that of the Alur, and of various decentralised societies like the Jopadhola

---

[53] Bithub Kenya, *Report on the African Blockchain Opportunity Crowd-Sale Campaign* available at http://bithub.co.ke/opportunity/?wpam_id=1).

[54] Garrick Hileman, "The Bitcoin Market Potential Index" papers.ssrn.com/sol3/papers.cfm?abstract_id=2752757.

[55] Justice, Law and Order Sector, *Criminal Justice Baseline Survey* (Kampala, 2002).

and the Karamojong, creates complications for policy makers and regulators. For a start, there are ideological conflicts between the rationales of customary system and Uganda's received legal system regarding conceptualisation of ownership of property, liability and recompense. In some communities, collective responsibility may be assumed for the harm done by the offender, and for the offender's rehabilitation. Such a traditional system may favour restorative penalties and achieving social equilibrium which include the opportunity for social learning or a re-examination of important values and socio-economic conditions of the community. The penalties may involve ritualistic and therapeutic intervention. Above all, social norms and justice are achieved through a participatory approach that uses a blended notion of legislative, judicial and executive power.

By contrast, Uganda like most former British colonies applies largely English rules of equity, and natural justice. Here, human rights law is the yardstick by which any regulatory measure or law is assessed to ascertain its legitimacy, proportionality and whether it achieves fair outcomes. However, the ways in which this public law interacts with the private law of localised ethnic societies is complex. Take the example of legitimacy. At the local level, communities might define legitimacy, not in legal terms of legal principles of legality, but in a relational context in which proportionality and just outcomes are premised on the value of the community and relationships, and where individual rights may be abridged for the common good.

So how might we engender a regulation that is culturally legitimate, premised on communal norms and participatory approaches, and where the yardstick might be different? We could start by understanding the ways in which each localised community might conceptualise law/regulation and how in their value system such regulation or measure is judged to be legitimate, proportionate and to achieve a fair outcome to that community. This means a move to a different type of type of yardstick- one that is based on relational values of justice such as equal participation and reconciliation. Regulation that does not engage with localised concepts of fairness, neutrality and procedural legitimacy may lead to aggrieved consumers taking complex cryptocurrency disputes to their traditional courts instead of the formal courts.

While using traditional courts may reflect an individual choice of jurisdiction on the part of the complainant, procedural justice in a formal sense may be compromised by the way in which customary courts conceptualise individual rights as a claim that can be restricted for the common good. Studies in countries like India that have leap frogged and adopted payment technologies, show that some of the most vulnerable consumers of payment technologies are women – they are more likely to be less educated, may be targeted deliberately by fraudsters and they may use the technology incorrectly. Would these localised traditional systems offer a safe space where women's issues can be resolved? It depends on the type of mechanism. In some societies, women's interests may be accommodated by offering a safe space for women perhaps through women only courts, or by having women representatives sitting on the court. With regard gender equality in representation, as research studies have shown, women may not have the confidence to fully participate or speak up in these proceedings and even then may speak only when asked to speak due to patriarchal norms.

Do localised traditional systems need some sort of guidance on how to deal with disputes arising from payment technologies? I think so. My own research found that kinship courts were happy to work with the government, but they accuse the government of interfering with their proceedings on the claims that they violate the law. Traditional leaders demand respect for

their jurisdiction given that legislative attempts to take away their (largely criminal) jurisdiction have failed. Given that fact that a significant portion of our people live in rural areas, and will increasingly use distributed ledger technologies, we need to take their concerns seriously.[56]

The potential use of the Blockchain to pay funeral expenses called '*kika*', or '*mabugo*' is a case in point. The ownership of funeral funds (given to the bereaved family) can be contentious given that misappropriation of funeral funds can take place at the hands of rogue individuals who receive the money on behalf of the bereaved families, or on behalf of their clans. In a typical clan setting, the aggrieved family (or clan) may well resort to kinship courts to seek redress regarding the stolen funeral funds. However, proof of who received the money (usually via mobile money) and in whose custody the money is, could lead to all sorts of accusations. In order for kinship courts to ask the right questions – about ownership, transfer and receipt of funds, the Blockchain with its distributed public ledger could provide valuable information to verify the transfer of funds to the recipient.

The Blockchain could also bring transparency to the transactions in the Savings and Credit Cooperative Organisations (SACCOs).[57] Recently, a group of people in Tororo complained to me that they were misled into believing that the money that they pooled together in their SACCO was meant for the immediate benefit of their families. They were later informed that the money was meant to cover future funeral expenses incurred on the death of the contributor. The community now worry that they have lost their money. Surprisingly, none of the aggrieved parties have reported this matter to the police or to the nearby magistrate's court. Rather, they are considering how to deal with this loss of funds in their own way, including asking friends or relatives in Kampala to help them recover the money. These developments indicate a loss of confidence in the state's investigate and adjudicatory system, but also in their own cultural system which appears to be inadequate to address the problem. This may be the same fate that befell Nsubuga when he lost the Bitcoins for his tuition fees to an unscrupulous merchant.

In order to engage with these communities who closely adhere to their norms and procedures, we need to appreciate the African perception of currency in a relational sense. Such an understanding calls for in-depth ethnographic studies on how communities conceptualise intangible or digital currency, and how they deal with disputes arising from misuse or fraud relating to such currency. Examples include cases of misappropriation of funeral funds paid in cryptocurrency. We could then draw on these studies to help develop regulations in this area. There are benefits and risks to integrating non state norms into regulation. The benefit of having a cultural transformation through closer integration of non-state norms and practices is that more consumers may choose to report cybercrimes like cryptocurrency fraud to their traditional bodies, to the formal institutions, or both. Whichever forum they choose, the systems would accommodate relational values of community and participatory justice within the society which they are familiar. This integration requires an acknowledgement of the failures or risk of the formal system. The first is attaining cultural legitimacy particularly in

[56] Uganda National Household Survey 2012/13 established that in terms of spatial distribution, 77% of Uganda's population live in rural areas.

[57] These organisations have to be registered under the Cooperative Societies Act 1991, the Cooperative Societies Regulations 1992, and draft By-laws of the SACCO. The Act is due to be amended by the Cooperative Societies Amendment Bill 2016.

traditional societies of the acephalous or egalitarian sort that may not view the state as a legitimate body for rulemaking. Unless they are in full control of the process, acephalous societies may not perceive state-centric top down regulation as legitimate, but rather may perceive regulation as a take-over of their jurisdiction. Of equal importance is the preponderance of English in official correspondence in some peri-urban and rural areas where the local languages are dominant. Minimum use of local languages could lead to tightly knit communities disengaging from the regulatory environment, thereby resulting in less, not more integration.

Recommendation

Accommodating non state norms and practices requires an amendment to the constitutional instruments in order to recognise the jurisdiction of these kinship bodies. Regulators should also consider using dominant localised languages in order to engage people in the regulatory environment. Reconciling the state and non-state systems is definitely a work in progress.

PLENARY SESSION 3

Keeping pace with changing technology

Participants identified the challenge likely to be faced by policy makers and legislators namely the ability to keep pace with the fast changing trend of technology. Taking the example of the United Kingdom Computer Misuse Act, participants noted that the debates in the Hansard reflected how little was known at the time about offences like unlawful access to computers or about the use the criminal law of trespass to prosecute such cases. In a similar vein, despite the enactment of Uganda's Electronic Signatures Act, questions remain about things like the best signature that is needed- just a password, or an email? Also, section 26 of the Electronic Transactions Act provided that electronic transactions should be reversible, yet for cryptocurrencies once a transaction was made, it was irreversible.

Legislators, regulators, policy makers and legislative drafters needed to understand the nature of the technology, the trends in user adaption, and the aspects of tech use that needed to be regulated. A starting point was to consider whether regulation was needed at all. The next step at the level of law reform was to establish where the laws were at, because to state that cryptocurrency ought to be regulated was to legalise cryptocurrency. The two steps would enable a meaningful debate to take place in Parliament on ways in which the existing law could keep abreast with technological developments without being outpaced by the technology.

Data sharing

Participants acknowledged the need for a sector wide database of financial crime that includes cases that are reported to the police, as well as those cases that are handled by the courts and the outcome of those cases. The police database ought to be linked to other public databases in order to share information.

Choice of terminology for regulation

Participants observed that some words like 'invest' were being used interchangeably with the word 'currency' which appeared to be contradictory, given that a currency if viewed as a medium of exchange could fluctuate and go up or come down. An investment by contrast was a rather ambiguous term as it related to a specific product. In order to use the correct terminology in regulation all those terms needed to be clarified. Even from a basic financial accounting perspective, a currency was a liability of an issuer and held as a claim by the person who held the currency. For a cryptocurrency, there was need to define these terms, to determine who had liability, and which body would be responsible for oversight.

Increasing smart phone ownership

Uganda may be leap frogging into the technological age, but it does not seem that the technology is relevant given that most people are still using basic (dumb) phones with no reliable access to the internet. Research from Intermedia 2016 established that by June 2016, only 6% of mobile phones in Uganda were smartphones- hand held devices that run the iOS and Android operating systems which facilitate apps. So even though public bodies like the URA have developed consumer facing apps, they will not reach their target population if only 6% of the population have smart phones. Uganda still has some way to go if the number of people who can afford smart phones in order to get access to apps that run cryptocurrency ventures is to increase.

Making customary law applicable

Customary law is used widely in rural areas and in some urban communities, but legitimacy of regulation is buttressed by the over-arching principle of legality as enshrined in the constitution and related public laws.

Participants recommended that the legality principle should be broadened in order to include oral customary norms including sanctions. Socio-cultural legitimacy could then be built on ownership and transfer principles drawn from customary norms.

Sociology of regulation

The developments in Ugandan society over the past year (since 2016) show how fast people are learning about cryptocurrency and are benefitting from it. Still, the issue of regulation frightens some people, because they only perceive regulation in negative terms: as frustrating to investors, and faulting everything a start-up company wants to do- in sum, an interference with peoples' lives. Such a negative perspective clouds an individual's ability to view the positive ways in which society could organise itself to harness the benefits of this technology.

It is important to note that it is the ordinary people who are not so sophisticated who actually control the economy at the informal level. Such ordinary people take risks in business and are ready to trust people. The ordinary people know where to find opportunities to make money and know where that money is – in this case in cryptocurrency. Although they are willing to

take the risks to get this money and make a profit, they fear regulation. This may be because of the way in which regulations are implemented. For example, it is not uncommon for bank staff to talk about a customer's financial wealth in the banking hall. This unethical behaviour exposes that individual to potential dangers of theft (or worse) from those who may overhear this conversation. At least with money tied up in cryptocurrency, nobody should know about it, except for the wallet provider or company with whom a person has dealings.

Regulations are very important, but those using or dealing in it need to understand what the regulations are, why they are necessary and what they mean for the development of the society. That way, ordinary people may buy in to the regulation and may better appreciate the value of regulation. Still, in making regulations, policy makers should remember that the criminals are always ahead of the regulator, and that the criminals always look for a way to evade regulations.

Closing Speech: Mr John Kisembo, Director of UNAFRI

I wish to thank all participants for coming here to discuss this important issue of cryptocurrencies. At UNAFRI, we are a crime prevention institute; we do research and training and offer advisory services to governments. We hope, that all of you here as regulators, policy makers and most importantly, the Law Reform Commission, will support our work by implementing today's recommendations. Many workshops have taken place here (as I said, our role is advisory), but implementation of recommendations has been a problem.

One of UNAFRI's area of interest is in national crime trends. We have hosted a crime statistics workshop that examined the lack of a unified crime report of Uganda. We found that the various agencies like the Police force, the Uganda Revenue Authority and the Directorate of Citizenship and Immigration Control all handle criminal cases, but the department specific information is not compiled together to form a national crime report. We hope this issue will be taken up.

This problem is replicated at the stage of domestication of regional conventions and protocols. At the national level, many African states sign regional conventions and protocols which they do not domesticate or ratify. Without the ratification of treaties into law, it is difficult for states to apply them at the national level. Without laws setting out obligations and rights, it is difficult to blame the law enforcement agencies like the police for not enforcing law and order because they do not have the laws to underpin their action.

The digital economy has ushered in the danger of cybercrime yet most African States are lagging behind in fighting cybercrime. Cybercriminals have taken advantage of this lacuna to wreak havoc on our communities. Still, UNAFRI is open to all activities that can improve the criminal justice system and we are ready to host events here. We have a digitised library and invite you to use our website. We open up a compendium of experts for each of our research areas and we are happy to offer training or technical advice. So when we come knocking on your doors, please open the door for us, come and join us.

UNAFRI look forward to seeing all of your organisations take responsibility for making sure that these proposals are actually enforced and not just left to gather dust. As a lead agency, you can rely on us to follow up how these recommendations and those that were passed on

the 6th July 2017 at the first round table on cryptocurrency control are implemented. We shall look forward to see what happens in the Parliamentary Committee on Accountability (PAC) because when the regulators meet the cryptocurrency and blockchain start-ups and businesses, we expect some tension between the two. The tension will be similar to what we have seen when the traffic police and taxi drivers meet. Taxi drivers are told not to park in restricted areas and where there are regulatory signs, but the taxi drivers decide to park in those places anyway. The enforcement agencies then need assistance to enforce the regulations. We expect a clash, but it will be a very good clash and all of us will benefit from it.

Crime prevention is about networking and building synergies with partner agencies. We appreciate the growing bond that has developed between the University of Birmingham Law School and UNAFRI. It is our wish that this partnership between us will continue to develop and flourish for the benefit of our region. Let us continue the tradition that has been established that every July, we can reach out to an even larger group in the regions of Africa.

Declaration on Fundamental Principles on the regulation of cryptocurrencies and the Blockchain (Digital Ledger Technologies) in Uganda and its Follow Up

Adopted by the participants at the 2nd Round Table on the Regulation of Cryptocurrency, held at the United Nations African Institute for the Prevention of Crime and the Treatment of Offenders (UNAFRI), Kampala, 6th July 2017

Preamble

Whereas the Roundtable recognises the importance of disruptive payments technology (Fintech) that includes cryptocurrency and its underlying technology- the Blockchain as a possible cost effective method of enabling micropayments in our developing economies;

Whereas the Roundtable recognises that Uganda's economy is agro based, has low levels of digital literacy, has economically disempowered populations particularly in rural communities, and requires a culturally appropriate socio-economic regulatory regime for cryptocurrency and related Blockchain technologies that ought to promote innovation while offering robust consumer protection;

Whereas the increase in the use of cryptocurrency and the Blockchain in the modern networked Africa constitutes a significant challenge to the regulatory capacity to respond to the socio-cultural, legal, economic and political effects of this emergent environment of disruptive payments technology;

Whereas the Central Bank of Uganda, policy makers, financial regulators and legislators should pay special attention to the protection of cryptocurrency users and consumers, while encouraging national efforts aimed at resolving the problems posed by disruptive payments technology including cryptocurrency and the Blockchain;

Whereas innovation of payments technologies is essential but not sufficient to ensure equity, social progress, and the financial inclusion of the unbanked and the economically disempowered; innovation confirms the need for the policy makers, financial regulators and legislators to promote effective and strong culturally appropriate policies, based on a rules-based but principled approach to regulation;

Whereas it is urgent, in a situation of growing disruptive payments technology, to reaffirm the immutable nature of the fundamental principles and rights embodied in the Constitutional, legislative and policy arrangements of African States and to promote their application within the technical rules based sphere;

The Second Round Table on Cryptocurrency regulation

1. Recalls that in being part of UNAFRI, of the African Union, and of other regional bodies like the African Development Bank, the Association of African Central Banks, and the

Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), Uganda has endorsed the principles and rights that underpin these regional unions;

2. Recalls that Uganda has undertaken to work towards attaining these principles and enforcing these rights basing on the nation's resources and dependent on its specific circumstances;
3. Recalls that these principles and rights have been expressed and developed in the form of specific rights and obligations in Regional Conventions like the Constitutive Act of the African Union, the African Charter of Human and Peoples' Rights, the Abuja Treaty establishing the African Economic Community, and the African Union Convention on Cybersecurity and Data Protection; regional level policies like the East African Community regional intellectual property policy; national constitutions and legislations; as well as in national sector specific regulation like the Bank of Uganda Consumer Protection Guidelines 2011- all of which are recognised as fundamental in African states;
4. Recalls that Uganda has taken the lead in East Africa in passing legislation on the regulation of e-commerce like the Electronic Transactions Act 2011, the Electronic Signatures Act 2011, and related laws like the Computer Misuse Act 2011- all of which aim to protect important principles and rights in e-commerce;
5. Recalls Uganda's commitment to improve her competitiveness through Information Communication Technology (ICT) development in its Uganda Vision 2040; and the National Development Plan II (NDPII, 2015/16-2019/20).
6. Declares that Uganda, even if she has not ratified some relevant Regional Conventions like the African Union Convention on Cybersecurity and Data Protection (2014), has an obligation arising from the very fact of membership in the African Union, in the Association of African Central Banks, as well as membership in ESAAMLG, in UNAFRI and in related bodies; to respect, to promote and to realise in good faith and in accordance with the regional Conventions, the Constitution of Uganda, legislation like the Bank of Uganda Act 2000, the Uganda Communications Act 2013, and other instruments; the principles and the fundamental rights which are the subject of those legal and policy frameworks and which include:
   (a) Principles on the collection and processing of personal data and on the processing of sensitive data;
   (b) Protection of the data subject's rights;
   (c) Principles of technological neutrality;
   (d) Principles of social justice;
   (e) Rights and freedoms including the right to privacy, to property, to freedom of expression, and to economic, social and cultural development;
   (f) Principles of non-discrimination, of participation, of equity and of gender equality; and
   (g) Recognition of the individual's duty to family and to society.
7. Recalls the resolutions of the 1st Cryptocurrency Roundtable of 2016, held in Kampala at UNAFRI on 7th July 2016 in which it was agreed that principles were required to underpin:
   i. Technological considerations in the regulation of payments technologies;
   ii. Policy approaches to the regulation of crypto currencies and the Blockchain;
   iii. Legal approaches including questions of legality; rights and duties; and consumer protection;
   iv. Conceptual approaches to defining cryptocurrencies;
   v. Ethical considerations when engaging with payment technologies;

vi. Investigatory, prosecutorial and judicial approaches to digital forensics and analytics, and capacity building; and
vii. Socio-cultural issues surrounding consumer behaviour especially among rural and illiterate African communities.

8. Recognises the obligation on UNAFRI to assist its Members, in response to their expressed needs, by making full use of its constitutional mandate and of its technical resources in accordance with Article II of the UNAFRI Statute by:
    a. Offering technical cooperation and advisory services to promote the ratification and implementation of the Regional Conventions and instruments;
    b. Assisting those member states that are not yet in a position to ratify some of these Conventions, in their efforts to promote and to realise the principles and fundamental rights which are the subject of these Conventions and instruments;
    c. Supporting member states in their efforts to create a supportive regulatory sandbox type environment for disruptive payment technologies (Fintech) and for digital ledger technologies in general, and for the specific use of cryptocurrencies and the Blockchain; and
    d. Working in collaboration with policy makers, legislators, financial regulators, private sector, civil society and academia to achieve the conducive regulatory environment.
9. Recognises the lack of clarity of policy objectives and the lack of rationalisation of policies among financial regulators which gap could undermine any efforts to engender conceptual clarity surrounding cryptocurrency and the Blockchain, and could weaken efforts to promote fair competition, ethical behaviour among Fintech, data security, data protection, social cultural relevance, and legality;
10. Recognises the gaps in the constitutional and legislative mandate of the Central Bank of Uganda and related financial regulators to clarify the place for cryptocurrency and the Blockchain in Uganda's emergent Fintech economy;
11. Recalls that the Warnings issued by the Central Bank (14th February 2017) on the need for the public to beware the risks of investment in Onecoin, underscores the risks to the public including to their data security and privacy;
12. Observes that the Central Bank Warnings could be strengthened to give clarity on the obligations of cryptocurrency businesses towards investors, consumers and the public;
13. Decides that, to in order to give full effect to this Declaration, a multi-sectoral follow-up ought to be implemented in accordance with the principles specified in the annex below, which principles shall be considered as an integral part of this Declaration;
14. Underscores the need for a principled approach to the regulation of digital ledger technologies, but stresses that the principles outlined in the Annex below, should not be used to stifle innovation or to replace technical rules, and states that nothing in this Declaration and its follow-up shall be invoked or otherwise used for such purposes.

ANNEX

FOLLOW-UP TO THE DECLARATION

Overall Purpose

1. The aim of this follow-up is to consolidate the efforts made by the participants to the first and to the second Round Tables to develop principled guidance that promotes the fundamental principles and rights enshrined in the international, regional and national laws and regulatory frameworks, and integrates the Resolutions of the First Round Table on cryptocurrency regulation (July 2016) that are reaffirmed in this Declaration.

2. In line with this objective and adopting the recommendation of the Central Bank of Uganda at this second Roundtable, this follow up will allow the establishment of a Working Group. The Working Group will identify areas in which collaboration on the development of policies and laws, and on the conduct of research studies may prove useful to the participating institutions and individuals in order to help them develop principled regulation of disruptive payment technologies based on these fundamental principles and rights. The Working Group comprising participants at both Round Tables, is not a substitute for the established legislative and regulatory mechanisms, but will merely offer expertise and guidance in a collaborative manner.

3. The regulation of disruptive payments technology (Fintech) - inclusive of cryptocurrency and the Blockchain, should be directed at trusted financial intermediaries who handle consumers' money via investment, who engage in money transmission services, who offer currency exchanges, and who offer mobile money and related services. A proportionate risk based technologically neutral approach that is both principled and rules based is recommended in order to encourage innovation and to offer consumer protection.

4. The principles set out below are based on existing practices of dealing with cryptocurrencies and the Blockchain; on the current policies, regulatory mechanisms, and the legal frameworks; and on the fundamental principles and rights that have informed the deliberations of the Round Tables of 2016 and 2017.

PRINCIPLES

1. **Automating regulatory compliance principles:** encourage the automation of regulatory compliance (reg-tech) underpinned by the principles of interoperability between traditional and Fintech payment systems, scalability, cybersecurity, accountability, transparency and trust. The starting point is a sector wide risk assessment similar to that carried out by the Financial Intelligence Authority. Regulators should also consider how encryption and other tech enabled protections could be drawn upon to offer effective consumer protection.
2. **Non-regulation of the Blockchain:** given the benefits of adapting the block chain technology to current payment systems like mobile money and traditional banking systems, such as widening financial inclusion through faster and transparent consumer focused micro-payments, the government should not regulate the Blockchain. However, further research on the benefits and risks of the Blockchain should be undertaken.
3. **Technological neutrality principle:** in the drafting of legislation, technologically neutral language should be used say in the definition of technologies. The courts of

law are encouraged to apply technological neutrality as a tool of interpretation- one that ensures that an Act or a Statute is interpreted or applied by the courts in such a manner that it does not favour or discriminate against any particular form of technology.

4. **Ethical principles** of 'do no harm', of fairness, of transparency, of trust, of non-deception (accurate description of the product) and of non-discrimination in the supply of products should underpin the obligations of consumer facing cryptocurrency and Blockchain businesses. Ethical principles may be achieved through sector specific liability laws like the Consumer Protection Bill 2014 and the Competition Bill 2014, with the aim to encourage socially desirable business behaviour and to protect consumers. An ethical approach by cryptocurrency users should underpin the regulation, and should strongly encourage cryptocurrency users to meet their tax obligations in order to stem the use of cryptocurrency as an off shore tax evasion scheme.
5. **Data security principles:** consumer protection should be underpinned by legal principles on the processing of personal data and the processing of sensitive data, as well as data acquisition using real time information.
6. **Data protection principles:** the data subject's rights inclusive of data privacy, the right to challenge decisions made on a purely algorithmic basis, the right to erasure, explicit consent and so forth, should be allocated by the draft Data Protection and Privacy Bill 2015. The use of Regulatory Sandboxes as a safe environment should be promoted in order to encourage innovation, but without jeopardising consumer protection.
7. **Legality principle**: the overarching legal principle is one of legality as enshrined in Uganda's constitution. The legality principle should be broadened in order to include the oral customary norms and sanctions.
    a. Legality also can be achieved through the application of existing laws like the Value Added Tax Act Cap 349 to transactions that use cryptocurrencies; through amendments to existing laws like the Bank of Uganda Act 2000 in order to delineate the relationship between fiat currency and cryptocurrencies; by harmonising legislation like the Financial Institutions Act 2004 and its associated Regulations, the Tier 4 Microfinance Institutions and Money Lenders Act 2016, and the Micro Deposit Taking Institutions Act 2003, in order to include cryptocurrency businesses in its scope; through the enactment of new laws like the Consumer Protection Bill 2014, the Competition Bill 2014, the Anti-Counterfeiting Goods Bill 2015, and the National Payments Systems Bill (drafted in 2016 by the Uganda Law Reform Commission)- which set out the obligations of providers, the rights and duties of all parties.
    b. Prospective legislation could build on existing guidance like the Bank of Uganda's Consumer Protection Guidelines 2011.
8. **Clarity:** the definition of payment technologies (Fintech) including cryptocurrencies should be based on the principle of clarity and certainty surrounding the qualifying and non-qualifying technology activities including the place for the Blockchain and related digital ledger technologies; when the change of business requires notification to authorities or requires pre-approval; and clarity surrounding the process of listing and the standards for listing for example on the Uganda Stock Exchange. Clarity and certainty is also required on the rules by which tokens like Initial Coin Offerings will be valued; on exemptions to licencing; on the interaction between cryptocurrency and fiat currency- for example as a medium of exchange or a store of value; on the agencies responsible for enforcement and oversight; on compliance requirements including

capitalisation and proof of solvency; on the tests and sanctions for non-compliance; and on the safeguards that are in place for investor protection and consumer protection. Clarity is also required on the public interests to be protected in regulation.

9. **Proportionality principle:** compliance requirements should pass the proportionality test by which the purpose for regulation of cryptocurrency is legitimate, the means by which the regulators objectives are pursued are laid down in the law, the regulatory intervention (measure) is correctly directed to its technological target, and the regulatory measure does not exceed what is necessary to attain the legitimate objective. Regulatory measure would include any proposed security bond. Equally, the sanction should be proportionate to the purported infringement. In this regard, the Know Your Customer and Anti Money Laundering requirements like suspicious activity reporting should not be so onerous as to stifle the innovation of start-ups.
10. **Policies** that aim to regulate cryptocurrencies and related payments technology should be underpinned by the following:
    a. **Principles of social justice** that aim to ensure a balanced economic development that supports innovation, interaction, and collaboration. This principle is encapsulated in Uganda Vision 2040. Such development could be achieved through a 'leap frog' approach to harnessing the benefits of payment technologies, and through incentive-based policies that encourage compliance with regulation for example through tax breaks or government subsidies.
    b. **Principle of sustainability and functional equivalence in policy goals**. Policy goals should aim for consistency and rationality with existing policies like the Monetary Policy; Fiscal Policy, Taxation policy, Consumer Protection and Competition Policy, National Trade Policy, ICT Policy and the Communications Policy, as well as with East Africa and the African regional monetary policy integration initiatives.
        i. Policy goals ought to take into account the difficulty of defining what is functionally the same aspect to be regulated and the need to draw on customary African frameworks for sustainability and for the inclusion and the protection of the economically disempowered.
        ii. The harmonisation of policies and laws (existing and prospective) should follow sub regional collaborative initiatives like the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), and continent wide developments like the work of the Association of African Central Banks on the harmonisation of monetary policy.
    c. **Principles of co- regulation** between the public and private sector (fintech), that avoids regulatory arbitrage, and over regulation.
    d. **Principles of a risk based approach** that clearly communicates the identification, selection, and prioritisation of risks as well as the rationale for that choice. The policy should be responsive to the principles of proportionality outlined above.
    e. **A Rights based approach** that recognises the right to economic, social and cultural development, to freedom of expression (to protect the production and distribution of software), and the right to property including intellectual property rights. Other rights include equal participation, equity, and gender equality.
    f. **Principles of social cultural legitimacy** that recognise legitimate cultural differences among the different ethnic groups, like the individual's duty to family

and to the society, the recognition of relational principles of ownership and transfer of property in emergency situations, participatory approaches to dispute resolution in close knit kinship communities, and the diverse range of ethnic languages spoken in a given district or region.

11. **Principles of extra territorial jurisdiction:** the legal and regulatory frameworks should be underpinned by principles of jurisdictional non-territoriality, reciprocity and mutual co-operation.
12. **Cross cutting capacity building** in investigation, adjudication, prosecution, cybersecurity and related areas should be based on principles of national, regional and international cooperation; on knowledge exchange of expertise; on ownership by the key stakeholders; on sustainability of the training programmes; and on work based learning.

Dated 6th July 2017, Kampala, UNAFRI

Comments or queries on matters raised in this Roundtable discussion report and the accompanying Declaration, may be directed to Dr Maureen Mapp at M.O.Mapp@bham.ac.uk.

Participants at the Second Round Table (6th July 2017)

Central Bank of Uganda

Mr Stephen Mulema,
Director, Financial Markets
Central Bank of Uganda,
Plot 37/45 Kampala Road, P.O.Box 7120, Kampala,
Website: www.bou.or.ug

Ms Christine Alupo,
Director, Communications
Central Bank of Uganda,
Plot 37/45 Kampala Road, P.O.Box 7120, Kampala,
Website: www.bou.or.ug

Mr Haruna Mukalazi,
Senior Principal Banking Officer
Central Bank of Uganda,
Plot 37/45 Kampala Road, P.O.Box 7120, Kampala,
Website: www.bou.or.ug

Mr Daniel Ocakacon,
Senior Principal Banking Officer,
Central Bank of Uganda,
Plot 37/45 Kampala Road, P.O.Box 7120, Kampala,
Website: www.bou.or.ug

Ms Cynthia K.A Sekirembeka,
Senior Principal Banking Officer
Central Bank of Uganda,
Plot 37/45 Kampala Road, P.O.Box 7120, Kampala,
Website: www.bou.or.ug

Mr Victor Walusimbi,
Head, Knowledge Management
Central Bank of Uganda,
Plot 37/45 Kampala Road, P.O.Box 7120, Kampala,
Website: www.bou.or.ug

Cryptocurrency Evolution Limited
Mr Ivan Kintu
Cryptocurrency Evolution Limited
Mukwano Courts, Kampala

Financial Intelligence Authority- Uganda
Ms Esther Kagira Aikiriza
Manager, International Relations and Strategic Analysis
Financial Intelligence Authority (FIA- Uganda)
Rwenzori Towers (Wing B), 4th Floor, Plot 6, Nakasero Road
Kampala, Uganda, P.O Box 9853, Kampala.
Website: www.fia.go.ug

International Federation of Women Lawyers (FIDA-Uganda)
Ms Julie Olule,
Programme Officer
International Federation of Women Lawyers (FIDA-Uganda)
Plot 100 Lutaya Drive, Bukoto, Kampala
P. O. Box 2157 Kampala, Uganda,
Website: https://fidauganda.org/

Judicial Training Institute (JTI) – Uganda
Dr Gladys Nakibule Kisekka**,**
Deputy Registrar Research and Law Reporting
JTI, Plot M105, Kinawataka Road, Mbuya 1
P.O. Box 7085, Kampala,
Website: http://www.jsi-uganda.org/

Makerere University School of Law
Dr Ronald Kakungulu-Mayambala,
Senior Lecturer
Makerere University School of Law,
P. O. Box 7062, Kampala,
Website: http://www.law.mak.ac.ug/

National Information Technology Agency – (NITA-Uganda)

Mr Emmanuel Mugabi,
Manager, Information Security Operations
National Information Technology Agency – (NITA-Uganda),
Palm Courts, Plot 7A, Rotary Avenue, (Former Lugogo Bypass),
P.O. Box 33151, Kampala, Uganda,
Website: http://www.nita.go.ug/

Ms Caroline A. Mugisha,
Manager, Regulation and Compliance
National Information Technology Agency – (NITA-Uganda),
Palm Courts, Plot 7A, Rotary Avenue, (Former Lugogo Bypass),
P.O. Box 33151, Kampala, Uganda,
Website: http://www.nita.go.ug/

Mr Baker Birikujja,
Legal Officer
National Information Technology Agency – (NITA-Uganda),
Palm Courts, Plot 7A, Rotary Avenue, (Former Lugogo Bypass),
P.O. Box 33151, Kampala, Uganda,
Website: http://www.nita.go.ug/

Press

Mr Joseph Kato
News writer/Reporter
Daily Monitor newspaper
Monitor Publications Limited
Plots 29-35, 8th Street, Industrial Area
P.O. Box 12141; Kampala, Uganda. Website: www.monitor.co.ug

Mr Sam Obbo
Media Consultant
P. O. Box 11291, Kampala

Mr Sammuel Sebuliba
Reporter, KFM/Dembe FM
Monitor Publications Ltd
Plots 29-35 8th Street, Industrial Area
P.O.Box.12141 Kampala-Uganda
Website: http://dembefm.ug/

Mr Benson Tumusiime
News writer/Reporter,
Red Pepper Newspaper (Uganda)
Website: http://www.redpepper.co.ug/

Sekabanja and Company Advocates
Mr Kato Sekabanja,
Managing Partner
Sekabanja & Co. Advocates
Commercial Plaza, 4th Floor, West Wing
Plot 7, Kampala Road, P. O. Box 2064, Kampala
Website: www.seklegal.com

Uganda Christian University Mukono, Law Faculty
Dr Anthony C. K. Kakooza,
Dean, Faculty of Law,
Uganda Christian University
P. O. Box 4, Mukono, Uganda
Website: http://ucu.ac.ug/

Uganda Communications Commission
Mr Julius Mboizi,
Senior Officer, Legal Affairs
Uganda Communications Commission
UCC House Plot 42 – 44, Spring road, Bugolobi
P.O. Box 7376 Kampala, Uganda
Website: www.ucc.co.ug

Uganda Law Reform Commission
Ms Lillian Kiwanuka,
Senior Legal Officer
Uganda Law Reform Commission,
8th Floor, Workers House, Plot 1 Pilkington Road, Kampala,
P. O. Box 12149, Kampala
Website: http://www.ulrc.go.ug/

Uganda Police Force
Mr Dan Munanura, Assistant Commissioner of Police,
Director, Electronic Counter Measures Department,
Directorate of Information and Communication Technology,
Uganda Police Force, Kampala. Website: http://www.upf.go.ug/

Uganda Revenue Authority

Ms Dorothy Nakyambadde,
Supervisor, Research and Planning Division,
Uganda Revenue Authority
P.O. Box 7279, Kampala, Uganda,
Website: https://www.ura.go.ug/

Mr Solomon Rukundo
Lawyer,
Uganda Revenue Authority
P. O. Box 7279, Kampala, Uganda
Website: https://www.ura.go.ug/

United Nations African Institute for the Prevention of Crime and the Treatment of Offenders (UNAFRI)

Professor E. P. Kibuka
Researcher,
Naguru, P.O. Box 10590, Kampala, Uganda
Website: http://unafri.or.ug

Mr John Kisembo
Director, UNAFRI
Naguru, P.O. Box 10590, Kampala, Uganda
Website: http://unafri.or.ug

Mr Patrick Mwaita
Programme Officer, Research and Training
UNAFRI, Naguru, P.O. Box 10590, Kampala, Uganda
Website: http://unafri.or.ug

Mr Christopher Mutyaba
Administrative Assistant
UNAFRI, Naguru, P.O. Box 10590, Kampala, Uganda
Website: http://unafri.or.ug

Ms Sarah Musoke
Administration and Finance
UNAFRI, Naguru, P.O. Box 10590, Kampala, Uganda
Website: http://unafri.or.ug

University of Birmingham
Dr Maureen O. Mapp,
Birmingham Law School, University of Birmingham,
Edgbaston, Birmingham
B15 2TT, West Midlands, England
Website: http://www.birmingham.ac.uk/schools/law/index.aspx

White- Mare Technology Ltd

Mr Ben Okello Mwaka, IT Developer
White- Mare Technology Ltd
2nd Floor, Victoria House, Kitintale

P.O. Box 31460, Kampala
Website: www.white-mare.technology

Ms Esther Kisakye, Administrator
White- Mare Technology Ltd
2nd Floor, Victoria House, Kitintale
P.O. Box 31460, Kampala
Website: www.white-mare.technology