REPORT OF THE FIRST ROUND TABLE DISCUSSION TO DEVELOP INSTRUCTIVE GUIDANCE ON THE REGULATION OF CRYPTO CURRENCIES IN UGANDA 7th July 2016

Virtual currency regulation in Uganda

Dr. Maureen Mapp ▸ University of Birmingham Law School ▸ Convenor

On 7th July 2016, the first ever Round Table discussion on policy, legal, ethical and socio-cultural issues surrounding the regulation of virtual currencies took place at the United Nations African Institute for the Prevention of Crime and the Treatment of Offenders (UNAFRI) in Naguru, Kampala. The event was convened by Dr. Maureen Mapp of the University of Birmingham Law School with the support of the Central Bank of Uganda, UNAFRI, and the African Centre for Cyberlaw and Cybercrime Prevention (ACCP) located at UNAFRI. The event was sponsored by the University of Birmingham Law School and the College of Arts and Law, as well as UNAFRI.

The aim of the discussion was to create awareness about the use of virtual currencies in Uganda; to share findings of the Commonwealth Virtual Currencies Survey (2015) on Uganda; to compare individual and institutional experiences; and to develop instructive guidance on effective ways with which to regulate this new form of crypto currency in Uganda.

The Kampala event drew participants from the parliamentary service, academia, financial investigatory and regulatory bodies, Chamber of Commerce and Industry, private Fintech advisory companies, and the insurance sector. Panelists came from UNAFRI, Makerere University College of Law, Economic Policy and Research Centre, National Information Technology Authority, Financial Intelligence Authority, Uganda Police Electronic Counter Measures Department, University of Birmingham, and Bitreco Limited – a Ugandan Bitcoin exchange.

Guiding principles that aimed to underpin any legal or regulatory framework were drafted by participants along thematic lines of technology, policy, law, investigatory, prosecutorial and adjudicatory issues. Participants underscored the need for comprehensive policies and strategies and awareness-raising among the public, the private sector and among rural communities. The principles will be further developed at the next meeting, in line with Uganda's laws and existing policies on finance, the economy, monetary matters, on information communication technology and cybersecurity.

This report covers the panel talks, discussions, recommendations and the draft guiding principles. The second roundtable event is scheduled to take place in July 2017.

Session 1: Virtual Currencies in Uganda. Opening statement by Mr. Patrick Mwaita, UNAFRI

The day began with an opening statement by Mr. Patrick Mwaita on behalf of UNAFRI and the African Centre for Cyberlaw and Cybercrime Prevention (ACCP). Mr. Mwaita welcomed participants to the first ever discussion on the regulation of virtual currencies which he hoped would influence digital economic developments in the East African region. He introduced Dr Maureen Mapp-a Fellow of the ACCP, Teaching Fellow in Law at Birmingham University and convenor of the Round Table discussion. Dr Mapp's research and teaching interests in crypto currencies inspired her to host the round table discussion in Kampala at UNAFRI to UNAFRI's delight. Mr Mwaita invited participants to engage in the discussions on the questions surrounding the regulation of virtual currencies in Africa.

Welcome Address. Dr. Maureen Mapp

Dr Mapp welcomed participants to the event. She thanked UNAFRI, Birmingham Law School and Birmingham College of Arts and Law for their generous funding in hosting the event. She also acknowledged the technical advice given to her by the Central Bank of Uganda.

The rationale for the event arose from two factors. First, as a module leader for Elements of Cyberlaw module on the Masters of Laws degree, Maureen had noted the dearth of African academic literature and scholarship in this area. Birmingham had a vibrant Africa Hub that aimed to integrate African related learning and teaching resources into curricula. The sources shared during the meeting would feed into the Cyberlaw curriculum and enrich it with contemporary information from the Africa continent. The second reason was that a cultural transformation of cyber legislation was necessary if Africa was to make its laws relevant to localized communities. The Round Table discussion was the first step towards this transformation.

The intended outcomes of the discussion were:

- The creation of an Africanist Think-tank on technological, policy, pluralist, ethical and legal issues that inform and influence the regulation of crypto currencies. The Round Table participants would become members of the Think Tank;
- Engagement in critical discourse on the regulation of cryptocurrencies through discussions and the publication of individual or institutional research publications such as policy papers, working papers, and research papers; and
- The development of instructive guidance based on principles of a multi-disciplinary nature.

Session 1: Understanding virtual currencies - Dr Maureen Mapp

The session began with an overview of virtual currencies and its contested definitions. For ease of reference, a working definition that drew upon that offered by the Financial Action Task Force (FATF 2014) was used in which virtual currencies were viewed as a digital representation of value that had no legal status but could be digitally traded. Functions of such currency included acting as a medium of exchange; a unit of account; and/or a store of value. Given the plethora of decentralised virtual currencies like Litecoin, Ripple, Etheruem, zerocoin and Bitcoin, the focus on Bitcoin, was because it was a cryptocurrency of choice for conducting a range of transactions in Africa including in Uganda,

South Africa, Nigeria (the Igot Bitcoin exchange) and Ghana (the Kitiwa exchange).

Dr. Mapp outlined the main players in the Bitcoin ecosystem including developers, miners, merchants, wallets and users of Biotin. The Bitcoin and its underlying technology-the Blockchain, facilitated creativity and innovation in financial payments due to the absence of a third party intermediary, relative cryptographic security of transactions, and the Blockchain's ability to facilitate micro payments and micro transactions. The Blockchain was of relevance to countries like Uganda that suffered from high levels of financial exclusion and under provision. Virtual currencies could therefore offer some level of financial inclusion to those excluded from the banking system (African Banker Magazine, May 2016).

Dr. Mapp presented the highlights of a survey that she conducted in 2015 for the Commonwealth Secretariat. The survey findings could be found in the Report of the Commonwealth Working Group on Virtual Currencies (Commonwealth Secretariat, 2016). Drawing on online sources and social media, the survey established that Bitcoins were being used in Uganda largely by individuals, charities and businesses, albeit in a regulatory vacuum. Bitcoin was not a fiat currency under the Bank of Uganda Act 2000, or the Foreign Exchange Act 2004. There were neither primary nor secondary legislation governing its use. Equally, there was no policy, strategies, interpretive guidance, or opinion to govern its use or to mitigate any risks.

Considering whether Ugandan policy makers, legislators and the public should be concerned about the risks posed by the Bitcoin, Dr Mapp pointed to research by Daniel Moore and Thomas Rid (*Cryptopolitik and the Darknet* 2016) that identified subcategories of illicit finance on the Dark Web. The sub categories were: Bitcoin-based methods for money laundering; trade in illegally obtained credit cards and stolen accounts; and trade in counterfeit currency. Examples of criminal activity on the Dark Web included the infamous case of Ross Ulbricht who founded a lucrative online drug marketplace called Silk Road but was convicted in 2015 for money laundering, computer hacking and conspiracy to traffic narcotics (*United States v Ross W Ulbricht* Case Number: S1 14-cr-00068-KBF-1). Ulbricht was now serving a life sentence in America. In addition, some of the features of Bitcoin like speed, scalability and resiliency were not absolute (CITI, 2016).The Ethereum digital currency hack in June 2016 worth between $45 million and $77 million was a case in point.

These concerns were echoed around the world. The European Banking Authority (EBA) warned of over 70 risks posed by the Bitcoin (EBA, Opinion addressed to the Council of the European Union, the European Commission and the European Parliament 2014). Elsewhere, the Crown Prosecution Service of the United Kingdom (UK) had requested the House of Commons for Restraint Order powers to deal with seizure of virtual currencies. Their arguments were that the UK's Proceeds of Crime legislation had nothing on the seizure of virtual currencies, and case law could not be used to compel the conversion of a virtual currency into physical money (CPS Submissions to Commons Select Committee inquiry into proceeds of crime, May 2016).

The response of public regulatory bodies was mixed. Bangladesh and Russia had been reactive and banned the use of virtual currencies. In Singapore and Norway, Bitcoin had no currency status and was considered a commodity. In the United States of America some entities like the Inland Revenue Service viewed Bitcoin as a taxable property, while in Michell Espinoza's case (possibly the first money-laundering prosecution involving Bitcoins) the judge ruled that Bitcoin did not qualify as money (July 2016). Elsewhere, the European Commission announced its intention to include Bitcoin and other digital currencies in the 2016 European Union (EU) anti-money laundering regulations. The EU rules

would require digital currency platforms to monitor transactions and users the same way that banks did.

On the African continent, most Central banks like the Bank of Uganda had adopted a 'wait and see' approach. This approach gave no guidance or strategy on the ways of harnessing the benefits of virtual currencies in expanding the digital economy while mitigating associated risks. While some like the Ghanaian and Nigerian Central Banks were considering regulation, others had cautioned against the use of virtual currencies. A case in point was Kenya, where the Central Bank issued a public notice on virtual currencies (CBK Public Notice 2015). The notice stated that the Central Bank did not view virtual currencies such as Bitcoin as legal tender as they were not issued by the Central Bank, lacked security and offered no protection in the case of failure. The Bank urged the public to desist from transacting in Bitcoin and similar products. The previous year, the South African Reserve Bank had issued a similar caution about risks posed by virtual currencies and the Block chain technology (South African Reserve Bank Position paper, 2014).

Despite the cautionary approach of Central Banks in Africa, states would do well to heed the recommendation by the Commonwealth Working Group on Virtual Currencies to improve their legislative and regulatory frameworks in order to protect the legitimate use of virtual currencies and to prevent cybercrime (Commonwealth Working Group on Virtual Currencies 2016).

One opportunity was the extension of Uganda's economic policy programme to 2017 by the International Monetary Fund under the Policy Support Instrument (PSI) arrangement. Uganda's current economic policy programme included the amendment of the Bank of Uganda Act, and the improvement of productivity in key sectors of the economy. Dr. Mapp argued that the PSI extension offered Uganda an opportunity to review existing policy and legislative instruments surrounding the use of virtual currencies in order to reap the benefits of Bitcoin and the Blockchain technology, while paying attention to any potential risks.

In the absence of a clear legislative and regulatory framework or guidance, Dr Mapp identified some useful starting points for the development of a rational regulatory framework. These included the Anti-Money Laundering Act 2013; the Bills of Exchange Act Cap 68; the Foreign Exchange Act 2004 and its associated Forex Bureau and Money Remitters Regulations 2006, the Income Tax Act 1997; the Insurance Act Cap 213, the Securities Central Depositories Act 2009, the Stamps Act Cap 342 and the Stamps Amendment Act No 12 of 2002.

The presentation concluded with three thematic areas for consideration:

Categorisation of decentralised virtual currencies (cryptocurrency)

- Are virtual currencies a currency, a commodity or security; taxable property, a negotiable instrument or bill of exchange, or some other digital entity?

Rights and interests of parties

- Should the state protect the rights and interests arising from this peer to peer transaction?
- If so which rights and interests should be considered: property rights, contractual rights, economic rights, transactional or any other right?

Policy, Strategy, Law, guidance, opinion

- Can law and regulation ever be socio-culturally appropriate?
- Challenges of legitimacy, legality, necessity, and proportionality of the measures?
- Evidential burdens and related investigatory, prosecutorial and adjudicatory challenges.

Session 1: Regional engagement in virtual currency regulation

-Mr John Kisembo, Ag Director, UNAFRI

Mr Kisembo welcomed the participants to UNAFRI and began by giving an overview of the functions of the institute. He explained that researching on virtual currencies fell within the remit of the Cybercrime project of the African Centre for Cyberlaw and Cybercrime Prevention (ACCP). The project was initiated at the opening of the Centre in 2010. The ACCP is located at UNAFRI.

Mr Kisembo underscored the importance of the regulation of virtual currencies in the African region. Bitcoin, the Blockchain and the related processes of development, mining and use of Bitcoins raised potential transnational and extra-jurisdictional concerns relating to illicit criminal activities. As such, it was necessary to gain a regional perspective on the scale of the problem as individual countries did not have the capacity to go it alone. That way, national efforts to regulate and legislate on virtual currencies would lead to collaboration at the regional and sub regional level.

Given that approximately 90 per cent (90%) of low-value transactions in Africa were in cash (Africa Business Investment News, BizNis Africa, July 8, 2014), it was conceivable that at some point, digital transactions would become the standard and at a low cost. This was possible given the growth of electronic devices like smart phones (World Economic Forum (WEF) Global Information Technology Report 2016, Global Pew Research 2016) in the African region. Even without the burden of regulation, pertinent questions remained about the threats posed by illicit criminal activities for which existing crime prevention systems and criminal justice models were ill suited to handle.

Mr Kisembo posited that the influence of virtual currencies could extend even further due to its use as an investment vehicle and its ability to spur the growth of an underground industry of violence-based and potentially harmful businesses. He expressed caution about fully embracing the use of virtual currencies without a risk assessment. In Africa, one of the areas of concern is the threat posed by virtual currencies to the security of nations and to the stability of national economies. As policymakers struggled to catch-up, efforts to develop an appropriate regulatory regime for virtual currency were at a critical juncture. Developing a risk assessment however, required national authorities in Africa to study the impact of virtual currencies in countries like the United States of America, the United Kingdom, and the European Union where regulatory measures were operational.

Moving forward, Mr Kisembo pledged the support of UNAFRI towards the promotion of the round table dialogue and the sharing of expert knowledge and best practices in order to inform the development of policy, legislation and regulations in Africa. This support would be through regional and international collaborative initiatives, research conducted under the auspices of the African Centre for Cyberlaw and Cybercrime Prevention, and support for the use of safe and easy-to-apply digital resources.

Such measures would necessitate the development of a coalition of agencies that would work to protect communities from the problems associated with virtual currencies. In addition, region wide programmes would be developed to build capacity on the use of virtual currencies, while addressing issues of cybercrime prevention.

In conclusion, Mr Kisembo hoped that the Roundtable discussion, premised on the good will of participating institutions and individuals, would initiate a process to develop a proactive intervention to inform the proposed policy, legislative and regulatory measures.

Session 1: Plenary Discussion

Participants began with a vote of thanks to UNAFRI for hosting the event, and to Dr. Mapp for convening the roundtable discussion which enabled a frank debate on a matter of great economic and financial importance in the African region. The discussion then turned to the potential challenges that could arise in any attempt to regulate virtual currencies.

Need for awareness raising

Participants identified the lack of knowledge among the public (including among some of the participants) about virtual currencies. Most people's understanding of currency was one of legal tender that was issued by a government with an established process of circulation, storage and exchange. Monetary transactions were physical and visible, and as such more easily understood by the general population. Fiat currency was also necessary to create economic stability.

Virtual currencies, by contrast were intangible, cross border by nature, and seemed to operate out of a 'spiritual' world. Mining- the basis on which the virtual currency value was determined; the risk of fraud and theft; and the level of protection accorded to users and other parties posed regulatory challenges to regulators. Yet, key regulatory and supervisory bodies like the Central Bank did not seem to have ready answers to these problems. Given that the lack of knowledge could potentially undermine the efficacy of virtual currency- awareness-raising was an imperative.

Need for further research into Virtual Currencies

Participants noted the need for research into the benefits and risks of using virtual currencies in the local contexts. The research would help give direction to the policy formulation, as well as regulatory and legislative processes.

In the midst of difficulties brought about by a distorted financial sector, the banking industry was having difficulty in regulating mobile money transactions. A weak financial system would not ably handle the digitisation of financial payments and related innovations. Moreover, a report by the United Nations Economic Commission for Africa (UNECA) established that the African region was losing about fifty two billion US dollars ($52 billion) annually in capital flight through money-laundering and related illicit online fraud (UNECA, High-level Panel on Illicit Financial Flows from Africa report, 2014; and Africa Capacity Report, Capacity Imperatives for Domestic Resource Mobilization in Africa, 2015). In addition to all these unregulated outflows, the innovation of (unregulated) virtual currencies would worsen the situation further, meaning that Africa could incur further losses.

A proposed solution was to develop policy that drew on research and on the work of key stakeholders in the public and private sector. On such policy, the foundation of a fair regulatory mechanism would be laid.

Slow pace of policy development

Concerns were also raised about the slow nature of policy formulation up against the fast-growing digitisation of financial payment and related commercial systems. The slow process could stymie innovations, but equally it could hinder the fight against cybercrime. It was conceivable that disruptive trading platforms like some on the Dark Web could create a parallel financial system that could pose a threat to the economic and financial stability of a state, yet fail to offer protection to consumers.

Low levels of computer literacy

In Uganda, about 15% of the population was computer literate and furthermore; their use of computers was largely limited to routine applications such as accessing emails. In order to put in place a regulatory framework for a largely unknown entity – the Bitcoin- there was need to acknowledge the low levels of computer literacy.

Moreover, if the 15% computer literate population were not well informed about virtual currencies, then rural communities were much more vulnerable, given their lower computer literacy levels. This meant that the adoption of virtual currencies by the rest of the population was some way off.

Dispute settlement

The lack of an intermediary like a Central Bank raised questions about the avenues for settlement of disputes among parties. Quite unlike the banking sector where the inter relationship between corresponding banks provided diverse cross border resolution mechanisms, the absence of an equivalent regulated mechanism for virtual currencies was an area of concern.

Session 2: Policy considerations

Mr. Arnold Mangeni, National Information Technology Authority

Mr. Mangeni gave an overview of NITA and of its regulatory mandate. He explained how NITA's work related to virtual currencies. NITA, a government regulatory body under the Ministry of Information Communication Technology was established in 2009 with a mandate to regulate and coordinate the development of information technology within the social economic context of Uganda. NITA put into effect the government's plan to automate and digitise transactions. Within its mandate, NITA regulated online payments like mobile money, mobile banking, credit and debit card transactions, and cryptocurrencies like the Bitcoin.

The underlying legal framework comprised three pieces of cyber legislation. The Electronic Transactions Act 2011 supported online transactions including payments, while the Electronic Signatures Act 2011 provided for the authentication of electronic signatures. The Computer Misuse Act 2011 aimed to prevent (among others) the unauthorised use of computer systems. An example of a potential unauthorised use was the claim in 2013 that criminals had hacked into the Uganda Revenue Authority vehicle registration database in order to forge vehicle registration number plates. This claim was denied by the Uganda Revenue Authority (*New Vision* and *Daily Monitor* newspapers).

Mr Mangeni highlighted the advantages of using virtual currencies for online payments. Such advantages include the reduction in the cost of printing currency, the low cost of transactions due to the use of digital wallets, the protection against double spending, encrypted keys and relative anonymity. From a policy perspective, however, virtual currency posed challenges to macroeconomic stability as its creation, supply and use were difficult to regulate. For example, people making purchases using Bitcoins were difficult to trace, and having completed their transaction such users did not always meet their tax obligations.

The regulation of Bitcoins required an acknowledgment that crypto currencies would interface with fiat currency at some point. One possible method of regulation was at the point of currency exchange. The Foreign Exchange Regulations 2006 could cover such virtual currency transactions. Another form of regulation was through criminal laws like the Penal Code Act which could deal with counterparty risk from exchange failure, theft or fraud. The main problem was in relation to transactions under the Electronic Transactions Act where it could be difficult to get damages for items purchased with Bitcoins. Another challenge was the statutory requirement for disclosure of the physical address of the seller under the Electronic Transactions Act. Given the anonymous nature of the virtual currency

transactions in the digital economy, the verification of parties involved would be difficult. NITA could offer technological support in such circumstances, but ultimately the regulation of a virtual currency would fall under the purview of the Central Bank of Uganda.

The session ended with a video presentation on the Bitcoin ecosystem including the development, mining, use and exchange of Bitcoins by Mr Andrew Owor, of White Mare Technology Ltd.

Session 2: Plenary Discussion

Regulating Bitcoin exchanges

The participants queried the effectiveness of regulation in dealing with counterparty risk from exchange failure. This was more so because the owners of virtual currency exchanges were unknown, and some would not be willing to reveal their locations. Equally, there were many users who would not exchange their Bitcoins for fiat currency, but would just trade in Bitcoins only. The difficulty in tracing those people or bodies that used Bitcoins as a medium of exchange but did not declare any taxable income was another regulatory challenge.

Participants recommended the development of a policy on the regulation of virtual currency exchanges and taxation.

Co- regulation to deal with anonymity

Participants considered the ways in which anonymous users could be subjected to regulation in order to prevent illicit criminal activities and to protect the consumer. Could a system of voluntary registration and the revealing the details of one's operations work? From a tax and regulatory perspective, the regulator would need to know who held these currency exchanges and custodial wallet services/accounts.

Need to invest in technology and capacity building

The example of the successful Silk Road investigations in the Ross Ulbricht case underscored the need for investment in technology and investigative and related skills in order for the enforcement of the regulation to work. Equally, NITA had an important role to play in the transformation of Ugandans into digital natives who could use Bitcoin while being aware of its limitations.

Legal status of virtual currencies

Establishing the legal status of virtual currencies was viewed by participants as important, given its cross-border nature of operations and its ability to influence fiscal and economic stability. For that matter, the views of stakeholders such as Uganda Communications Commission (UCC), and telecommunication service providers were important to guide policy development.

Session 3: Economic and socio-legal issues

Virtual Currency and Monetary policy

Dr Ezra Muyandonera, Economic Policy Research Centre, (EPRC) Makerere

The session began with an overview by Dr Muyandonera of the benefits of adopting virtual currencies namely the promotion of financial inclusion, and the creation of financial efficiency. Virtual currencies offered fast, cheap and efficient means of facilitating a peer to peer exchange while reducing transaction times and costs. Beyond payments, virtual currencies and their underlying technology could facilitate accurate record keeping in a range of financial systems including stock exchanges, central securities and trade repositories. Through financial efficiency, the system could promote financial inclusion.

While acknowledging their benefits, Dr Munyandonera argued that virtual currencies posed challenges to monetary policy and to the Central Bank. The virtual nature of the currency meant that transactions could not be easily monitored by the Central Bank, yet such transactions could affect macro stability tools like the inflation rate. The digital nature of the virtual currencies made it difficult to gather statistical data about their operations. Equally, it would be difficult to distinguish licit from illicit transactions. Furthermore, the use of a distributed ledger to centralise online transactions appeared to eliminate the use of the Central Bank as a focal point in setting monetary policy.

The risk to Uganda's monetary policy was low at the present time. Still, if the 'digital natives' who used virtual currencies grew exponentially, then there were implications for policy and regulatory approaches. In relation to the latter, the diversity of the functions of regulatory bodies such as supervision, investigation, and prosecution meant that the optimal approach to virtual currency regulation was a multi-sectoral one. For although virtual currencies combined many attributes of the electronic payments, currencies and commodities, their multi-faceted nature was far broader than what could be covered under the powers of a single regulator. This called for effective policy coordination among the various regulators.

Any policy that was geared towards regulating virtual currencies would have to weigh the risks posed by its use, with the benefits of innovation in a budding digital economy. The adoption of virtual currencies in Uganda came at a time when Uganda was broadening its financial sector to embrace technological innovations. Therefore, over regulation could impede the adoption of virtual currencies and their underlying technology.

The main recommendation was for any regulation to aim to close the technological loopholes that facilitated abuse (like tax evasion and money laundering), that compromised financial integrity, and that exposed the consumer or investor to possible exploitation.

Session 3: Virtual Currency & law

Mr Ernest Kalibala, Makerere University School of Law (MUK)

SCHOOL OF LAW
MAKERERE UNIVERSITY

Mr Kalibala began with a brief introduction to the curricula of Makerere University Law School. He explained that the School offered an undergraduate course called *Computing and the Law* which was designed to investigate the intangible and tangible elements of computing and its interface with the law. Mr Kalibala then raised five areas that needed further clarification before the development of any law on virtual currencies could begin.

The first issue was clarity surrounding the status of virtual currency given that it was unclear when a monetary value attaches to it. A related question was whether the value of virtual currencies were based only on the computing/mining process, or also on hoarding which aimed to enhance value-rather like the *magendo* practice in Uganda in the 1970s when essential goods were hoarded due to scarcity. If virtual currency had a value, it was subject to price fluctuations. Arguably, these characteristics could also mean that virtual currency could be considered a property.

Consumer protection was the second area of concern. In traditional banking, there was a level of consumer protection offered through the system. For example, if a bank went bust, clients were entitled to some level of compensation. The problem with virtual currencies was the lack of consumer protection if the event of an exchange failure in the virtual currency markets, or

fraudulent dealings by merchants. The question in relation to the consumer protection system was to whom would a consumer have recourse in the case of a failed transaction? The risk was greater if a transaction was irreversible. Lack of protection was further exacerbated by the low levels of computer literacy and a relative lack of awareness about virtual currencies and computer protection laws.

The transnational nature of the currency meant that it was difficult to determine who would regulate the entirety of a transaction. Would states sign a treaty on cross border regulation; or set up an international body; seek support of the United Nations; or leave regulation entirely up to national agencies? Using an analogy from the banking sector, Mr Kalibala explained how the Bank of International Settlement set up the Basel Committee on Banking Supervision. The Committee developed Core Principles on Banking Supervision which provided a forum for cooperation on banking supervisory matters. Given the plethora of virtual currencies in operation, the questions surrounding ownership and jurisdiction made the creation of a similar benchmark for virtual currencies even more complex.

A wider discussion needed to be held on the aim of the regulation: was it regulation of an unlawful activity or determination of the lawfulness of an activity? These two situations required different approaches. Given the NITA presentation, it was clear that the discussion was geared more towards the regulation of a lawful activity. That being the case, while embracing the benefits of technological innovation, there was need to look into rights, responsibilities, protections and standard setting, and to be cautious about the risks involved.

Session 3: Cultural transformation of Virtual currency regulation-

Dr Maureen Mapp, University of Birmingham

In considering the need for a cultural transformation of currency regulation that suited the African communal context, Dr. Mapp examined the existing approaches, rationales and their limits before moving on to the foundations on which a culturally appropriate regulatory mechanism for Bitcoin use could be developed.

An examination of the current regulatory approaches showed that a state controlled regulatory approach was not necessarily suited for Africa's local context. Tensions remained between the promotion of innovation, the protection of consumers' rights and maintaining stability in the financial sector. The important question of how to engender a cultural transformation that adopted an 'African' relational approach to property (including currency) remained largely unexplored.

The case for promoting innovation was uncontroverted because emerging markets needed low cost financially inclusive payments systems. Crypto currencies had gained traction in Africa because they helped provide some level of financial inclusion to the computer literate and even to non-digital natives. Some African companies that operated in Bitcoins included Bitpesa of Kenya, Beam of Ghana, Bitstake of Nigeria and BitFinance of Zimbabwe (Gabriella Mulligan, Biz Community, 2015).

Previous speakers had highlighted the need to protect consumers from fraud, theft or exchange failure. Their arguments were equally valid. Virtual currency exchanges were usually unregulated and losses were rarely compensated. The failure to compensate victims following the collapse of the Mt Gox Bitcoin exchange was a case in point. In Uganda, the much tweeted experience of Mr. Ronald Nsubuga who received school fees in Bitcoins from his sister in the USA,

and was later conned of more Bitcoins by a rogue merchant in Kampala was another example. Existing consumer protection laws in Uganda did not adequately cover this scenario as legislative enactments and legal doctrines often predated (and rarely caught up with) technological developments.

Regarding stability in financial sector, it remained questionable whether virtual currencies threatened the Uganda shilling. This was more so because there was a lack of consensus on a universal definition of currency. Whether Bitcoin was viewed as currency depended on the context in which a claim/case was brought as the recent Kenyan case of *Lipisha Consortium Ltd and Bitpesa Ltd V Safaricom* Petition 512 [2015] eKLR illustrated. In *Lipisha*, the court ruled that Bitcoin represented monetary value (para 79) and that Safaricom was justified to suspend the services of Lipisha and Bitpesa Ltd, after Bitpesa dealt in Bitcoin without approval of the Central Bank of Kenya. Similarly, the European Court of Justice in C-264/14 *Skatteverket versus David Hedqvist* ruled that Bitcoin was a currency and therefore fell under the currency exemption for VAT purposes. In contrast, in the American case of Michell Espinoza- Espinozathe court ruled that Bitcoin was not the equivalent of money as it was not backed by any government or bank, and was not "tangible wealth".

The contested nature of Bitcoin as currency mirrored the lack of a universal definition of money. Some like A. Mitchell Innes argue that money was transferable credit supported by accounting, while others like G. David viewed money as any medium tangible or intangible, adopted for effecting payments. It was also questionable whether there were property rights in money (T. Cutts).

The need for state interventions in what was essentially a private peer to peer transaction was equally contestable. Crypto currency's tools for security and trust in open networks like encryption offered robust protection of information, including personal data, and a reduction of the impact of data breaches and security incidents. In such a situation there was no need for a law or regulation. This position could be challenged on the grounds that the use of encryption should not prevent national authorities from safeguarding important public interests like data privacy in accordance with the conditions and safeguards in the law. In short, there was need to carefully consider the suitability of a public law (as contrasted with private law) to enforce the rights associated with owning Bitcoins.

Rights associated with the Bitcoin raised pertinent questions surrounding the protection of private interests. It was not clear what rights are conferred to a person holding a Bitcoin, and against whom? Were these rights contractual, and to what extent was a Bitcoin a chose in action? It seemed that an investor did not have control over any Bitcoins, and could not force a website to give back Bitcoins. Equally, an investor only had a contractual right against the operator of the website, but this was not analogous with property rights (Shawn Bayern).

Answering these questions necessitated a policy and regulatory framework that prevented the excessive restriction of private rights like the right to data privacy or the right to property. There was need for clarity on the circumstances in which a justified interference of rights could be asserted *and* tested. Appropriate legal tests included:

- **Legitimacy of the aim:** was the measure aimed at protecting morals, public order, rights of others or some other pressing social need?
- **Legality of the measure:** was the measure accessible, precise and did it set out foreseeable consequences of one's action?

- **Necessity:** was the measure necessary, or could less onerous means have been used?
- **Proportionality:** was the measure proportionate to achieve the aim?
- **Balancing of rights**: were individual rights balanced with the rights of others?

These criteria were considered to some extent in the Kenyan case of *Lipisha* (2015). Safaricom was accused of violating the petitioner's right to a fair administrative process (fair hearing) by failing to give the petitioners adequate notice prior to the suspension of the services offered to the petitioners (para 65). Another potential violation of the right to property (para 81-83) was the withholding of money belonging to the petitioners' customers by Safaricom following the suspension. Safaricom argued that the measure (suspension) was legitimately aimed to subvert an illegality.

The petition was dismissed. The court found that none of the rights cited were violated. Rather the service was suspended for a period of time under the terms and conditions set out in the commercial agreement that had been accepted by all the parties.

Lipisha's decision was atypical of the legal conceptualisation and determination of rights. Even so, there was a need to include localised perspectives of rights in order to engender greater community engagement in the financial and banking system. Dr. Mapp urged the participants to begin to think about an African relational approach to property as inclusive of currency. This reconceptualisation was important given that people in the rural communities determined their ownership structure of property and the right to benefit, to harm or to prevent interference with the property, in accordance with the localised customs and ethical values. Communities also had their own 'court' systems and remedies for breach of customary laws (Owor, 2012 study on Jopadhola clan courts).

Ultimately, the ACCP, universities, all participating institutions and individual researchers needed to engage in cross disciplinary ethnographic studies. Such studies would help locate an African conceptualisation of currency, of responsibilities and interests, and of localised dispute mechanisms in the existing policy and regulatory frameworks. The research would hopefully lead to the development of policies and regulatory frameworks that were culturally appropriate to rural communities.

Session 3: Plenary Discussion

Bank of Uganda lack of regulatory powers over virtual currencies:

Concerns were raised about the legality of any regulatory action taken by the Bank of Uganda as the Bank of Uganda Act 2000 did not appear to give the Central Bank the powers to regulate virtual currencies. Participants specifically considered Section 5 on the formulation and implementation of monetary policy; Section 17 on monetary obligations or transactions being expressed, recorded and settled in the shilling as the unit of currency; and Section 23 on the issuance of legal tender. These provisions as well as any related subsidiary legislation did not give explicit regulatory powers over virtual currencies to the Central Bank.

Related provisions in the Uganda Constitution (Article 162) provided that the Bank of Uganda should (a) promote and maintain the stability of the value of the currency of Uganda; and (b) regulate the currency system in the interest of the economic progress of Uganda. Even so, participants observed that there was nothing in the Constitution that appeared to empower the Central Bank to regulate virtual currencies.

Given the growing innovation in virtual currencies, it was foreseeable that one day Uganda's currency could be backed by a 'Bit standard' instead of the gold standard; or be

valued in terms of a 'Bit currency' not the Uganda shilling. That being the case, there was need for specificity in the law regarding the legality of the Central Bank's powers to regulate virtual currencies.

Participants proposed that policy makers like the Ministry for Finance and Economic Development and other stakeholders including the Bank of Uganda needed to decide on whether the law should be amended in order to give the Bank the power to regulate virtual currencies.

Self-regulation and public interest

Virtual communities, it was acknowledged, were largely self-regulated as illustrated by organisations like the Bitnation. Bitnation aimed to offer a voluntary system of governance, but participants were not sure about the veracity of such mode of governance including safeguards to prevent arbitrary decision making, offer impartial adjudication and enforce recompense. This was an area that required further study more so because of concerns that some victims of exchange failure or fraud could be left without any compensation as happened in the Mt Gox scandal.

Participants concluded that state intervention was necessary in the public interest. Such views found support in the *Ssebaduka v Warid Telecom Limited* (Miscellaneous Application No. 204 of 2014, Decision of 20 August 2014), where the High Court stated that public interest included "having confidence that court will enforce reasonable breach of the law that balance the sanctity of business efficacy in a free market economy." Given the risks of financial instability that virtual currency could pose, it was recommended that public interest should not be ignored in any proposed regulatory framework.

Legislation does not support technological features

Uganda has enacted laws like the Computer Misuse Act that criminalised illegal online activities. Even so, participants noted that not all laws supported the core features of virtual currencies. For example, the Anti Money Laundering Act 2013 does not provide for a person to hold an anonymous account (AML Act 2013, Section 6 (a), (b)).

Participants recommended that laws ought to embrace the technological features of currencies.

No precedent from Mobile money cases

Despite their distinguishing features, mobile money was analogous to virtual currencies in the use of digital devices like smart phones to transfer money. Nonetheless, participants observed the lack of instructive guidance from court cases on the regulation of mobile money as exemplified by the case of *Abdu Katuntu and Kimberly Kasana v MTN Uganda and six others* HCCS No. 248 of 2012 (decision of 2015 by Judge C Madrama). There Katuntu and Kasana sought a declaration to have mobile money regulated under the Financial Institutions Act 2004 but lost on a technicality. The case was wrongly filed in the High Court (which lacked jurisdiction) rather than with a tribunal established by Uganda Communications Commission as stipulated in the Uganda Communications Act 2013.

Similarly, the two cases in which Ivan Ssebaduka challenged Warid Telecom (2013, 2014) led to no satisfactory outcome as the cases were lost at the preliminary hearing/ miscellaneous application stage.

Session 4: Financial intelligence and investigations

Mr Lazarus Mukasa - Financial Intelligence Authority (FIA)

Financial Intelligence Authority
Safe Money for a Secure Market

The session began with Mr Mukasa outlining the role of the Financial Intelligence Authority (FIA) that was established under the Anti-Money Laundering Act 2013 to ensure financial integrity through Anti money laundering (AML) and combating terrorism financing techniques. The FIA adopted a multi stakeholder approach premised on co-operation at the national, regional and international level.

Focusing on convertible cryptocurrency, Mr Mukasa acknowledged the benefits of its legitimate use like speedy efficient payment systems, reduction in transaction costs and transfer of funds, and the potential to promote financial inclusion and innovation. Even so, he cautioned that convertible virtual currency could be used to move value in and out of fiat currencies and the financial system, which presented potential money laundering and terrorism financing challenges.

Primarily, the anonymity of the internet based transactions that lacked face-to-face customer relationships permitted anonymous funding and anonymous transfers. The lack of affordable Anti Money Laundering (AML) software made it difficult for investigatory bodies to monitor and identify anonymous suspicious transaction patterns.

Fundamentally, the global outreach of virtual currency transactions meant that the responsibility for compliance, supervision and enforcement of AML and Combatting the Financing of Terrorism (CFT) remained unclear. This was because the customer and transaction records were sometimes held by different entities often in different jurisdictions, which made it difficult for law enforcement agencies to access. Worse still, the components of a virtual currency system could be located in jurisdictions that did not have adequate AML/CFT controls.

On the vexed question of regulation, Mr Mukasa noted the lack of consensus as to whether virtual currency should be subjected to some form of regulation by a government authority or an alternative entity. He explained that although Uganda did not have a specific regulatory framework for virtual currency, there was guidance from the Financial Action Task Force (FATF) aimed at helping public authorities and the private sector to identify and effectively address the risks of money laundering and terrorism financing associated with the use of virtual currencies.

FATF recommendations were that countries should consider applying the relevant AML/CFT requirements specified in the international standards to convertible virtual currency exchanges and institutions that acted as nodes. This was where convertible virtual activities intersected with the regulated real currency financial system. FATF Recommendations 1, 14 and 2 were regarded as useful starting points for Uganda.

FATF Recommendation 1 was that countries needed to identify, understand, and assess their own money laundering/and or terrorism financing risks including those risks associated with virtual currency and other new technologies. Countries had to take action aimed at effectively mitigating those threats.

FIA's proposal in this regard was to undertake a multi-stakeholder risk assessment of virtual currency products and services in order to gain a clearer understanding of how they worked in relation to each other, and what impact this had on the regulatory mechanisms of AML and CFT. In addition, there were other non ML/TF aspects of virtual currency including consumer protection, prudential safety and soundness, and network

security that required further investigation for potential risks.

According to FATF guidance in Recommendation 14, money or value transfer services (MVTS) operating in a country needed to be subject to monitoring for compliance with registration and /or licensing and other applicable AML/CFT measures. The registration and/ or licensing requirements could be applicable to domestic entities providing convertible virtual currency exchange services between virtual currency and real currencies.

FIA's proposal was to review Uganda's existing legislation to establish whether the activities of money or value transfer services (MVTS) that dealt in virtual currency complied with registration and licensing requirements. It seemed apparent that if such entities were involved in the transfer of money or value, then certain provisions in the Anti-Money Laundering Act, 2013 and the Foreign Exchange Act, 2004 would be applicable to them. Establishing the legality of the operations of these entities was of importance.

FATF Recommendation 2 called for national cooperation and coordination with respect to the development of AML/CFT policies involving the virtual currency sector. In this regard, FIA recommended the development of policies that took into account the following:

- The need for sensitisation of stakeholders on the emerging concept of virtual currencies;
- The development of a coordinated multi-stakeholder risk assessment;
- The development of a robust AML/CFT regulatory framework in relation to virtual currencies;
- A non AML/CFT policy that covered consumer protection, prudential safety and soundness and network security; and
- Stakeholder cooperation to be spearheaded by Bank of Uganda and to include the FIA, other regulators, and the legislative, investigative, and prosecutorial bodies.

Session 4: Investigations

Mr Bill D. Ndyamuhaki, Acting Assistant Commissioner of Police E-Security. Electronic Counter Measures Department. Uganda Police Force

Mr Ndyamuhaki began by outlining the work done by the Electronic Counter Measures Department, namely the investigation of cybercrime in general. The department also carried out computer forensics and network analysis. The presenter then gave an overview of the challenges faced by the police in investigating illegal activities that were associated with virtual currencies.

The lack of specific offences with which to charge offenders was the first challenge. The proliferation of money transmitting services like Money Gram and Western Union that transacted foreign exchange in Bitcoins posed problems for investigators as there was no law that specifically criminalised the exchange or receipt of money in Bitcoins. Also, it was not clear if the Bank of Uganda were able to regulate these sort of transactions. Similarly, the Computer Misuse Act 2011 did not criminalise acts associated with virtual currencies.

Mr Ndyamuhaki used the example of the MTN case to exemplify the limits of the law. In March 2015, some employees of the telecom giant MTN Uganda were prosecuted for fraudulently creating fictitious e-money to the value of 21 billion Uganda shillings. The money was to be withdrawn by participating mobile money agents. This fraud allegedly happened between 2011 and 2012. Mr Ndyamuhaki offered a possible explanation for the overturning of the initial conviction and sentence on appeal- the

inadequacy of the Bank of Uganda Mobile Money Guidelines (2013) which did not appear to address the increase of the supply of money beyond programmed levels by such companies.

Gathering information through Intelligence led policing was a second challenge. This model of policing relied on data collection in cyberspace sometimes through external partnership projects with institutions like virtual currency foundations and Bitcoin exchanges. The lack of technical expertise among investigators often meant that the suspects had more sophisticated hardware and software, and technical know-how. To counter this problem, the police needed to develop capacity and to acquire sophisticated tools for investigation.

Thirdly, jurisdictional problems arose from the transnational nature of cybercrime. The police had nonetheless used international co-operation with other police forces in the past with some limited success. A case in point was the counterfeit currency investigations, where the police traced the suspicious transactions of an American-Mr. Ryan Andrew Gustafson (alias Jack Farrel or Willy Clock) who was living in Uganda in 2013. Using intelligence led policing and working closely with the United States Secret Service, the Uganda Police unearthed a cyber counterfeiting scam on the Dark Web run by Gustafson from his home. Gustafson had created over $2 million US counterfeit dollars- most of it passed in Uganda and some of it in the United States of America. Gustafson was later extradited in 2015 to the United States of America where he is facing trial for currency counterfeiting (among other charges).

In conclusion, Mr Ndyamuhaki supported the proposition for further research into the legality of these activities. He also underscored the need for nation-wide awareness raising programmes to enable the public feed information to the police via social media and other online means. Strengthening technical capabilities meant that the police needed to train currency experts and more investigative analysts. Above all, some sort of guidance or regulation was needed, and clearly the Central Bank as a key stake holder had to take the lead on this.

Session 4: BITRECO

Mr Robert Kirunda – advisor to BITRECO Company

The last panelist was Mr Kirunda, a legal advisor to BITRECO- a Ugandan based cryptocurrency exchange and trading company. BITRECO he explained, did not mine Bitcoins but aimed to facilitate its use for payments and related transactions. In this respect BITRECO had its own Bitcoin Exchange portal called Binusu.com, its own governance structure, and legal services. The company's exchange operated at various locations in Kampala and issued Bitcoins at the prevailing exchange rate. The rise in the adoption of virtual currencies was driven in part by the success of the mobile money in rural parts of East Africa, and by the denigration of the capabilities of Bitcoin by those who had not appreciated its value to financial inclusion.

Basing on his experience of trying to get BITRECO registered in Uganda, Mr Kirunda shared his thoughts on the regulation of virtual currencies. The first problem was the practicality of regulating virtual currencies due to their widespread and instantaneous nature of transactions.

The second issue was Bitcoin's relative anonymity which enabled criminals move large amounts of money to transact illicit activities without raising suspicion. For example, in *Uganda Vs Hussein H Agade and 12 others* (Cr Sess Case No. 0001/ 2010, Judge A. Owiny Dollo's decision of 27 May 2016) on the 2010 twin bombings in Kampala, it was not clear where the money used to finance the terrorist bombings came from.

This showed how difficult it was to trace such transactions.

The lack of an intermediary or third party appeared to render the Bank of Uganda redundant because the supply and value of the Bitcoin was determined by the Bit community, not by the Central Bank. In addition, the level of mathematical sophistication involved in the computing of Bitcoins made it less susceptible to counterfeiting than when paper and ink were used. This computing element posed challenges to investigators who were used to tangible forms of counterfeit currency.

Despite these characteristics, Mr Kirunda was optimistic that the regulation of crypto currencies was possible given the fact that smart phones and similar devices were gradually permeating rural societies. The first step was to identify the key players in the entire Bitcoin ecosystem in order to know who to target. The players included the developers, miners, wallet providers, exchanges and merchants but each player had limited knowledge of the holistic details of the other. Targeting the wrong group would be futile as it could lead to arbitrary regulation that could stifle innovations.

The next step was to establish the sets of rights that needed protection like proprietary rights, intellectual property rights, privacy and the right to information. There was also a need to consider protection of the fiduciary relationship between lawyer-client.

Selecting a suitable approach mattered. Blocking the use of virtual currencies as was the case in Kenya was not an appropriate solution given the rapidly evolving nature of cryptocurrencies. Rather, a co-regulatory approach enabled the state to harness the benefits of Bitcoin and the Blockchain such as micro-low cost transactions that were cheaper to operate than mobile money. What mattered was the determination of the value of the Bitcoin.

The scope of any law had to be clear on what behaviour it aimed to control. The Anti Money Laundering Act 2013 for example, did not criminalise money laundering via commodities. The provisions on suspicious transactions were equally imprecise. A suspicious transaction under Section 1 of the AML Act 2013 was defined as one that was inconsistent with the customer's legitimate business or personal activities, or displayed a complex or suspicious transaction. Suspicious transactions included large sums of money that bore no relationship to the owner or their business (Section 9 AML Act 2013). The yardstick for determining the level of suspicion in the Act was vague.

Lastly, Mr Kirunda emphasised the importance of establishing co-operation between the police, regulators, the public and the online community in order to support intelligence led policing, and the AML/CFT mechanisms provided for under the law. Only by working together could the regulation be effective.

Session 5: Draft principles

The participants agreed to the development of instructive guidance underpinned by principles intended to preserve financial stability and legal certainty. The principles would be informed by academic research, scholarship and data from the financial regulators including banking, insurance and the finance sector.

The participants agreed to form a Think Tank to share expert knowledge and practice and to generate a body of research. In addition, international sources such as the African Union Convention on Cyber Security and Personal Data Protection (2014), the Commonwealth Computer and Computer Related Crimes Model Law (soon to be updated), the report of the Commonwealth Working Group on Virtual Currencies, the World Economic Forum Global Information Technology Reports, and the FATF guidance for a risk-based approach to virtual currencies were useful to

developers of policy, legal and regulatory frameworks.

The following draft technological; policy; legislative; investigatory, prosecutorial and adjudicatory principles associated with the regulation of virtual currencies were agreed:

1. Technological issues

1.1 **Security**: Network security, prudential safety and soundness, and cybersecurity strategies should underpin policy and regulatory frameworks.

1.2 **Trust**: any technological developments should aim to maintain trust in both the fiat and virtual currencies.

1.3 **Risk assessment**: regulators should undertake a multi-stakeholder risk assessment of virtual currencies in order to gain a better understanding of how specific virtual currency products and services interact with traditional financial and payment systems, and with each other. The risk assessment ought to establish what suspicious transactions look like.

2. Policy objectives

2.1 **Innovation, inclusion and economic stability**: any policy should aim to set standards that embrace the technological features of virtual currencies in order to support innovation and foster financial inclusion. In so doing, the policy should ensure that the creation, supply and use of virtual currencies supports macroeconomic stability through micro-low cost transactions.

2.2 **Policy development:** any policy development should take place in the short to medium term, and should draw on research, scholarship and data from industry.

2.3 **Consumer protection and security**: there is need for a non AML/CFT policy that covers consumer protection, prudential safety and soundness, and network security.

2.4 **Mitigating risks and abuse**: policy considerations should address the technological loopholes that compromise financial integrity/stability; expose the consumer to possible exploitation or fraud; facilitate abuse like tax evasion; and threaten national security.

2.5 **Protecting rights and interests**: Private rights and the public-private interests should be protected in every policy.

2.6 **Regulatory approach**: A co- regulatory approach should aim to bring together the virtual currency ecosystem and the regulators. The approach should draw on ethical values in Ugandan society.

2.7 **Awareness raising and increasing computer literacy**: new policies should draw or link into existing policies like that on the expansion of ICT and on increasing computer literacy levels. Policies should also aim to raise levels of awareness about the benefits of and the threats posed by the use of virtual currencies.

3. Legal framework

3.1 **Legality:** the legal status of virtual currencies in Uganda should be established by a constitutional or legislative amendment.

3.2 **Power of regulatory bodies**: the legality of the powers of the Central Bank and other regulatory bodies to regulate virtual currencies should be stablished by a constitutional or legislative amendment.

3.3 **Categorisation of virtual currencies**: the legal framework should determine if virtual currencies are a form of money, currency, commodity, taxable properties, bills of exchange, or negotiable instrument or some other entity. The question of ownership of the currency should also be considered-

namely whether it is private or public property.

3.4 **Rights, Responsibilities, Protections**: any proposed legal framework should set out the rights of parties including contractual rights, proprietary rights, property rights, intellectual property rights, data privacy rights and the right to a fair administrative hearing/fair trial. The law should also set out the responsibilities of parties, their liabilities including under the criminal law, protections (including consumer protection), and online mechanisms for the settlement of disputes.

3.5 **Legitimacy:** an African relational approach to property (and currency) is needed in order to engender socio-cultural acceptability of any proposed legal framework. The approach ought to encompass localised notions of the ownership structure of property, the right to benefit, or to prevent interference with the property. The law should also take into account the local customs, ethical values, dispute resolution systems and remedies.

3.6 **Interference with rights**: Any interference with individual rights should be weighed against the legal criteria of legitimacy, legality, necessity, proportionality, and the balancing of rights.

4. Investigation, prosecution and adjudication

4.1 **Capacity building:** the Police Electronic Counter Measures department need to invest in technology (hardware and software) and the training of experts to investigate cybercrime.

4.2 **Intelligence led policing:** a strategy for co-operation between the police, regulators, the public and the online community needs to be developed in order to support intelligence led policing and ensure compliance with AML/CFT mechanisms.

4.3 **Digital evidence**: Both the police and the Directorate of Public Prosecutions need to strengthen their methods of securing and adducing digital evidence, and negotiating evidential burdens.

4.4 **Jurisdictional and international co-operation**: in order to transcend cross border jurisdictional challenges, robust international co-operation strategies should be developed.

Next steps

A copy of this report will be made available to a wider audience on UNAFRI, University of Birmingham and other websites. Any feedback received will help to inform the agenda of the next round table discussion. The next event would include a wider range of stakeholders including from the Judiciary, law drafters, and other East African countries. The principles will be further developed at that event.

Comments or queries on matters raised in this RoundTable discussion report may be directed to Dr Maureen Mapp at M.O.Mapp@bham.ac.uk .

Participants

Mr. Ernest Kalibala,
School of Law, Makerere University,
Website: http://www.law.mak.ac.ug/

Prof. E.P Kibuka,
Researcher, UNAFRI, Kampala, Uganda,
Website: http://unafri.or.ug/

Mr. Robert Kirunda,
Kirunda and Wasige Advocates,
Website: kirundawasige.co.ug

Mr. Solomon Kirunda,
Department of Legal and Legislative Services, Parliament of the Republic of Uganda,
Website: http://www.parliament.go.ug/

Mr. John Kisembo,
Acting Director UNAFRI, Kampala,
Website: http://unafri.or.ug/

Mr. Arnold Mangeni,
National Information Technology Authority, Kampala, Uganda,
Website: http://nita.go.ug/

Dr. Maureen O. Mapp,
University of Birmingham Law School, UK,
http://www.birmingham.ac.uk/index.aspx

Mr. Lazarus Mukasa,
Manager Operational Analysis
Financial Intelligence Authority, Kampala
Website: www.fia.go.ug

Mr. Andrew Munanura,
Legal Counsel,
UNAFRI, Kampala, Uganda
Website: http://unafri.or.ug/

Dr. Ezra Munyambonera,
Senior Research Fellow,
Economic Policy Research Centre,
Makerere University, Kampala,
http://www.eprcug.org/

Ms. Sarah Musoke,
Administration & Finance Assistant,
(UNAFRI), Kampala, Uganda
Website: http://unafri.or.ug/

Mr. Patrick Mwaita,
UNAFRI and National Coordinator ACCP,
Website http://cybercrime-fr.org/index.pl/accp

Mr Charles Mutyaba,
UNAFRI, Kampala, Uganda
Website: http://unafri.or.ug/

ASP Mr. Bill Dickson Ndyamuhaki,
Electronic Counter Measures Department,
Directorate of Information and Communication Technology, Uganda Police Force
Website: http://www.upf.go.ug/

Mr. Martin Okumu,
Uganda National Chamber of Commerce and Industry, Kampala Uganda
http://www.chamberuganda.com/news/

Mr. Wilbrod Owor,
Managing Partner,
FINCON AFRICA, Kampala
Website www.finconafrica.com

Mr. Andrew Owor,
White Mare Technology, Kampala,
Website: www.white-mare.technology

Mrs Solomy Namakula Sekatawa,
(ICEA) General Insurance Company Limited
https://www.icealion.com/ICEA/index.php/home-ug

Mr John Sembuya Ssali,
Administration and Finance,
UNAFRI, Kampala, Uganda
Website: http://unafri.or.ug/

Dr. Mathias Ssamula,
Associate Professor,
Department of Sociology, Makerere University
Website: https://ss.mak.ac.ug/