MAKERERE LAW JOURNAL **MARCH 2021**

Volume 18 Issue 3

THE LEGAL RISKS OF CRYPTOCURRENCY ON STATE SOVEREIGNTY; A CASE STUDY OF UGANDA

Ntamugabumwe Victor and Joshua Kingdom

RECOMMENDED CITATION:

Ntamugabumwe Victor and Joshua Kingdom (2021), "The Legal Risks of Cryptocurrency on State Sovereignty; A Case Study of Uganda" Volume 18 Issue 3, Makerere Law Journal pp 118-152

THE LEGAL RISKS OF CRYPTOCURRENCY ON STATE SOVEREIGNTY; A CASE STUDY OF UGANDA

Ntamugabumwe Victor and Joshua Kingdom*

ABSTRACT

State sovereignty is conventionally known to mean that all states are equal under Public International Law, the decisive criterion being effective power over territory and people. Indeed, the most rudimentary definition of a state is the organization of power over territory and people within that territory. However, sovereignty today depends much on the state's monetary independence – the state's capacity to control the flow of money and currency in their jurisdiction. With the constant evolution of money transactions from Cash to credit and then to crypto, the state must always be ready for each revolution so that sovereignty is kept. Cryptocurrencies work outside the existing legal financial framework and as such avoid the state's invented structure to control their monetary policies, stability to achieve sovereignty.

1.0 INTRODUCTION

The world of money has increasingly evolved from time to time. It has moved from cash to cashless transactions over time. This has evidently been facilitated by the advancement in technology and the pursuit of a peer to peer cash transaction without middlemen.[1] On October 31, 2008 the pseudonymous Satoshi Nakamoto released his proposal for an electronic cash system known as Bitcoin.[2] This has opened up countless block chain systems known as cryptocurrencies which have gained popularity in the international community as a medium of transaction transcending current financial institutions and cross border regulation. A blockchain is a database encompassing a physical

* Special thanks to the Barry Ainomugisha, Kenneth Kiapi Kotura and the Makerere Law Journal Editors, your help during our preparation of this paper is duly noted.

1 Maria D, Guntram B. W. "The Economic Potential and Risks of Crypto Assets: Is a Regulatory Framework Needed?" Policy Contribution. Issue No. 14| September 2018.

2 Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (White Paper, Bitcoin 2008). 1 http://bitcoin.org/bitcoin.pdf [accessed 23 March 2021]

chain of fixed-length blocks that include 1 to N transactions, where each transaction added to a new block is validated and then inserted into a new block. When the block is completed, it is added to the end of the existing chain blocks.[3] As such blockchains are an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. This new blockchain technology in cryptocurrency has been noticed in Uganda as various cryptocurrency exchanges have opened up offices. These include Crypto Savannah[4], Binance, One Coin and others.

State sovereignty is conventionally known to mean that all states are equal under International Public Law.[5] The decisive criterion is effective power over territory and people. Indeed, the most rudimentary definition of a state is the organization of power over territory and people within that territory.[6] However, state sovereignty today depends much on the state's monetary sovereignty – the state's capacity to control the flow of money and currency in their jurisdiction.[7] Therefore, the control over money and finance determines monetary sovereignty, which, arguably, is the actual sovereignty.

In February 2017, the Bank of Uganda (BoU) issued a warning against the use of cryptocurrencies citing the absence of investor protection schemes and the relevant regulatory mechanisms.[8] The bank warned that the entity "ONE COIN DIGITAL MONEY" is not licenced by Bank of Uganda under the Financial Institutions Act 2004 and is, therefore, conducting business outside the

---

3 Joseph J. Paul R. BLOCKCHAIN. A PRCTICAL GUIDE TO DEVELOPING BUSINESS, LAW AND TECHNOLOGY SOLUTIONS. McGraw-Hill Education 2018 1st Edition

4 For More on Crypto Savanah, visit https://cryptosavannah.com/ [accessed March 23, 2021]

5 James R Crawford. Brownlie's Principles Of Public International Law. 8th Edition. Pg. 447

6 The so-called "three-element theory." See Georg Jellinek, Allgemeine Staatslehre (1905).

7 Robert A. Mundell, "Money and the sovereignty of the state." Columbia University.

8 Bank of Uganda. Warning to General Public about "One Coin Digital Money" operations in Uganda. Feb 14, 2017 http://www.bou.or.ug/bou/bou- downloads/press releases/2017/Feb/ Bank-of-Uganda-warning-on-One-Coin-Digital-Money-in-Uganda-pdf [accessed 23 March 2021]

regulatory purview of the bank and that "the public is strongly encouraged to do business with only licenced financial institutions. The bank also warned that "whoever wishes to invest their hard-earned savings in crypto currency forms such as Bitcoin, one coin, Ripple, Peer coin, Name coin, Doge coin, Lite coin, Byte coin, Prime coin, Black coin, or any other forms of digital currency is taking a risk in the financial space where there is neither investor protection nor regulatory purview."

Cryptocurrencies like Bitcoin challenge the post Bretton woods system of financial control on worldwide transaction.[9] The Bitcoin currency is decentralised and therefore is neither issued by any government nor is it stored in one location. They utilise a Distributed Public Ledger barring the need for a trusted third party such as a bank. With cryptocurrencies, mints do not print them, banks are not required to store cryptocurrency and escrow agents are unnecessary to verify transactions.

To many consumers, cryptocurrency appears to be a superior method of transaction in terms of efficiency and transaction cost. However, to the state, the removal of a trusted and regulated third party carries significant drawbacks concerning government's control of commerce.[10] This weakens sovereign state's capacity to protect their citizens from harm because they sidestep the regulations that monitor monetary transactions. This continuously reduces the government's legitimacy and thereby their fall.

During fiat[11] transactions, trusted third parties like banks, credit card companies and escrow agents restrict and report transactions with ties to

---

9 The Bretton Wood system was established by agreement in July 1944 with an aim to create international currency exchange regime. More importantly, this agreement established the International Monetary Fund and the World bank which still stand up to day decades after the Bretton Woods system collapsed. This is the system that introduced the modern-day financial frameworks. For more on this refer to. https://www.investopedia.com/terms/b/brettonwoodsagreement.asp last accessed on March 22, 2020 at 16:00 hrs.

10 Ryan L. Frebowitz, "Crypto Currency and State Sovereignty." Thesis. Naval Post Graduate School. Monterey, California. June, 2018

11 According to Investopedia, "Fiat Currency is a currency that a government has declared

criminal or terrorist entities. As a result, individuals and organisations transacting with fiat are required to register with a trusted third party. This is different with the Public Distributed Ledger transactions of cryptocurrencies.

Crypto currencies are an attractive means of fundraising for terrorists due to their anonymity. This does not take away the idea that the transactions stored in the public ledger provide an easy audit trail that traces the donations back to the source.[12] While bitcoin is still not a reliable source of fundraising for terrorists and jihadists, this may change in the near future due to a future potential acceptance of a new crypto currency offering more, or the creation of, online exchanges that do not adhere to the money laundering laws.

This will not be the first time the government of Uganda has had to deal with a technological advancement in money transactions like the current one. However, it will be interesting to see how it copes-up. Similar debates ensued when the state took to mobile money regulation following more than a decade of its existence.[13]

As such, there is need for a systematic regulation. A peer-to-peer transaction without a third party and without regulation would certainly lead to criminality and the loss of the legitimacy of the current system of government. If a government is incapable of regulating money transactions then it's a matter of time before unsupervised and unregulated transactions lead to criminality, loss of legitimacy and sovereignty.[14] This paper looks at viable ways under which cryptocurrencies can be regulated by the state and then offers recommendations for the same.

---

to be legal tender but it is not backed by a physical commodity." Fiat Money. Investopedia Nov 20, 2003. http;//www.investopedia.com/terms/f/fiatmoney.asp/ [accessed 22 March 2021]

12 Yaya F," The New Frontier in Terror Fundraising; Bitcoin." The Cypher Brief(blog) August 24, 2016.
Available at
http://ucscu.coop/index.php/media-centre/news/53-mobile-money-tax-proposal-may-have-a-negative-impact [Accessed 7th February 2021]

14 supra n4

2.0 CRYPTOCURRENCY - FROM WHENCE HAVE WE COME?

In order to understand how we come to a currency that uses cryptography, we shall go back in time to understand the need to use cryptocurrency. First though, a simple elaboration on what money actually entails.

2.1 What is money?

Money is any item or verifiable record that is generally accepted as payment for goods and services, repayment of debt and advancement of credit.[15] But simply put, money is just a medium of exchange, a unit of account and a store of value.

a) Money as a medium of exchange

Money acts as an intermediary between a seller and a buyer. For example, instead of exchanging accounting services for shoes, the accountant now exchanges accounting services for money. This money is then used to buy shoes. To serve as a medium of exchange, money must be very widely accepted as a method of payment in the markets for goods, labour, and financial capital.[16]

b) Money as a unit of account

Due to its ability to be a medium of exchange, money is also used as a unit of account. A unit of account is something that can be used to value goods and services, record debts, and make calculations. In other words, it is a measurement for value. A unit of account has three important characteristics relevant to money.[17] These characteristics include; - Divisibility, Fungibility and Countability.

---

15 Yuval N. H. MONEY – Vintage Minis. You may also refer to Wikipedia. Available at https://en.wikipedia.org/wiki/Money [accessed 22nd January, 2021]
PRINCIPLES OF ECONOMICS, Chapter 27 – Defining Money by its functions. Available at https://opentextbc.ca/principlesofeconomics/chapter/27-1-defining-money-by-its-functions/ [Accessed 25th January, 2021]

17 Available at

Divisibility requires that a unit of account can be divided so that its component parts will equal the original value. If you divide a shilling into four quarters, the total value of the four quarters still equals a shilling. Likewise, if you cut a bar of gold in half, the two pieces together will equal the same value as the original bar as a whole.

Fungibility requires that a unit is viewed as the same as any other with no change in value. A shilling is the same as any other shilling, and 12 ounces of 24-carat gold are not different from another 12 ounces of 24-carat gold. On the other hand, all real estate is unique, and diamonds vary by colour, cut, clarity, and carat.

Countability requires that a unit of account is also countable and subject to mathematical operations. You can easily add, subtract, divide, and multiply units. This allows people to account for profits, losses, income, expenses, debt, and wealth.

Therefore, for any money to count as a unit of account it must possess the above discussed qualities.[18]

c) Money as a Store of value

A store of value is the function of an asset that can be saved, retrieved and exchanged at a later time, and be predictably useful when retrieved.[19] Money has been one of the greatest stores of value due to its liquidity and stability. This is what guarantees a person to have savings and be sure that at the end when they want to spend those savings, they are worth what they saved or even more.

From the above discussion, it can be concluded that there are three functions of money; a medium of exchange; a unit of account; a store of value. In a cash

---

https://study.com/academy/lesson/money-as-a-unit-of-account-definition-function-example.html [accessed 26th January, 2021]

18 Mathias D and Martin S," Money as a Unit of Account." Econometrica Vol. 85 No.5 2017 Available at https://www.jstor.org/stable/44955172?seq=1

or credit-based economy, the above functions are what legitimise the money at function.

2.2 Barter Trade – Cash based and Credit Based systems

The earliest form of exchange was barter trade.[20] It worked on a very simple principle. If Victor wanted medicine and Joshua wanted food, they would just exchange the food for medicine and the transaction would have happen.

The transaction would also happen this way. If Victor has food that he is willing to trade for medicine. However, Joshua has the medicine but no need for food, but instead wants cattle, a meeting could be arranged with a third person who has cattle (Jane) and three would get what they want.

However, it should be noted that it was crucial to look for someone who had something that you needed and you had something they needed for the transaction to go through – the famous double coincidence of wants issue.[21] Two systems emerged to solve this issue of double coincidence of wants – Credit and Cash.

In a cash-based system, Victor would be able to buy the medicine from Joshua, and only sell the food to Jane later. From there, Jane can sell her cattle to Joshua.

In a credit-based system, Victor and Joshua would be able to transact. Victor would get the medicine but Joshua would get a favour owed to him. Victor would be in debt and therefore would get a new want - cattle. When Victor encounters Jane, they would trade cattle and food. Then Victor would go back to Joshua with the cattle to settle the debt.

---

20 Barter Trade was the earliest form of exchange in purchase of goods. Available at https://www.investopedia.com/insights/what-is-money/ [accessed 22 January, 2021]

21 Introducing Money available at https://courses.lumenlearning.com/boundless-economics/chapter/introducing-money/ [Accessed 23 January, 2021]

However, even when this evolution happened – barter trade was still affected by two things; Transferability and Divisibility. It was hard for example for Victor to quantify how much of the food he would need from John in exchange for cattle. So there needed to be an agreement to determine this problem and as such the trade would be tiring inefficient and confusing. Therefore, commodity money came into the picture.

Commodity money solved the problem since it was much more mathematical and easier to deal with. In Uganda one such commodity was cowry shells.[22] For instance, two cowrie shells would buy a woman for a wife in the ritual of marriage.[23] It is from this background that the evolution of money continued to minting of coins and then to the fiat currency that we see today.

2.3 Money and E – Commerce

Electronic commerce or e-commerce is a business model that lets firms and individuals buy and sell things over the internet.[24] This necessitates the use of credit facilities such as credit cards.

An online credit transaction necessitates the involvement of a number of intermediaries, to be successful. This will involve banks, credit card companies and other intermediaries.[25] As such, it is a credit-based transaction that will necessitate one surrendering their credit card details hence a record of their identity and the nature of the transaction(s). One such intermediary is Pay

---

22 Karin P. "Monetary Practices and Currency Transition in early colonial Uganda." The African Economic History Network. 18th July, 2016
Available at https://www.aehnetwork.org/blog/monetary-practices-and-currency-transitions-in-early-colonial-uganda/ [accessed 22 Jan, 2021]

23 When Two Cowrie Shells Could Buy a Woman? The East African Magazine. Available at https://www.theeastafrican.co.ke/tea/magazine/when-two-cowrie-shells-could-buy-a-woman-1293988 Last accessed on 25th January, 2021 at 08:00 hours.

24 Investopedia Definition.
Available at https://www.investopedia.com/terms/e/ecommerce.asp [accessed 26 January, 2021]

25 https://www.tutorialspoint.com/e_commerce/e_commerce_payment_systems.htm [accessed 26 January, 2021

Pal.[26] The intermediary and the vendor will settle the transaction at the end of the day.

This kind of transaction is different from a Cash-based system. In this system, transaction is by cash and there is no need for intermediaries. Therefore, the system guarantees anonymity, as a bank would track your expenditure in a credit-based system. When you pay in cash the vendor does not need to know who you and as such anonymity in as far as identity and nature of transactions will be quite guaranteed.

Since the 1990's very many companies have attempted to remove this risk of constant monitoring of people's transactions. We shall look at a few of these and what made them fail the attempt.

2.4 Fiat money and Currency.

Fiat money is government issued currency that is not backed by a physical commodity such as gold and silver, but rather by the government that issued it.[27]

- *How fiat money/currency works*

Fiat money or currency was introduced as an alternative to commodity money or representative money. The value for fiat money is derived from the relationship between demand and supply and the stability of the issuing government rather than the worth of a commodity backing it as it is the case for commodity money. It should be noted that fiat money has value only because the government controls that value and as such it lacks intrinsic value.[28]

---

26 For reference, visit https://www.paypal.com/ug/home [Accessed 27 January, 2021]

27 https://www.investopedia.com/terms/f/fiatmoney.asp [accessed February 8, 2021]

28 Corporate Finance Institute, "What is Fiat Money?" Available at https://corporatefinanceinstitute.com/resources/knowledge/economics/fiat-money-currency/ [accessed 8 February 2021]

Fiat currency is not supported by any physical commodity, but by the faith of its holders and virtue of a government declaration. acts as a storage medium for purchasing power and an alternative to the barter system. It allows people to buy products and services as they need without having to trade product for product, as was the case with barter trade. However, stability is key, and as such, there is need to control how much of the money is in circulation.[29]

- *Fiat money/currency and sovereignty*

Through the control of Fiat money and currency, its value and circulation – governments have immense control over and can monitor everything in the economy. Therefore, the control over money and finance determines actual sovereignty.[30] It should be noted that only countries that issue their own currencies retain control over their monetary policies, a precondition for monetary sovereignty, hence the right to exercise state sovereignty. This is certainly different from states that decide to adopt a foreign currency or join forces with others to adopt a new common currency. These give up the control of their monetary policies, stability hence loss of monetary sovereignty.[31] To this date real sovereignty of states has come from their ability to control their financial institutions under fiat currency.

2.5 How Cryptocurrencies Work

While this paper seeks to discuss the sovereignty of the state in the wake of crypto currency, it's pertinent to discuss and understand this technology with

---

29 Jason Hall, "Fiat Currency. What it is and Why it's Better than a Gold Standard." The Motley Fool. Available at https://www.fool.com/investing/general/2015/12/06/fiat-currency-what-it-is-and-why-its-better-than-a.aspx [accessed 8 February 2021]

30 Katharina Pistor, From Territorial to Monetary Sovereignty, Theoretical Inquiries In Law, Vol. 18, P. 491, 2017; Columbia Law School Center For Law & Economic Studies Working Paper No. 591 (2017). Available at "From Territorial to Monetary Sovereignty" by Katharina Pistor (columbia.edu)

31 See HYMAN P. MINSKY, The Financial Instability Hypothesis: An Interpretation of Keynes and an Alternative to "Standard" Theory, in Can "It" Happen Again? Essays On Instability And Finance 59 (1982) (originally published in 1977 on the tendencies of a financial system to destabilize endogenously).

basic technical issues. Cryptocurrency is a kind of digital money that is designed to be secure and, in most cases, anonymous.[32] It is mainly internet based and uses cryptography with blockchain. Crypto currencies work like any other money. As a medium of exchange – one can buy or sale goods using cryptocurrencies. However, one has to turn fiat money into cryptocurrencies in order to use them – for example as of February 9, 2021 a bitcoin cost 168,760,595.60 Ugandan shillings.[33]

- **The Road to 2008 – BITCOIN**

This Paper will rely on the Bitcoin ecosystem in order to explain how cryptocurrencies work. This is because of its market value popularity and being the first working cryptocurrency to have been created.[34] The domain name[35] was first registered on August 18, 2008. It was mainly a link to the Satoshi Nakamoto white paper that outlined bitcoin.[36] The major argument of the paper is that a purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution.[37] And after this we have come to see very many other cryptocurrencies commonly referred to as altcoins.

But where do the ideas behind bitcoin come from? What other payment systems preceded Bitcoin? What happened to them and more importantly what made them fail? This paper will give a few examples of failed systems to show where Bitcoin comes from.

---

32 Available at https://www.telegraph.co.uk/technology/0/what-cryptocurrency-why-how-work-bitcoin-ethereum/ [accessed 9 February 2021]

33 Available at https://www.google.com/intl/en/googlefinance/disclaimer/ [accessed 9 February 2021]

34 Available at https://bitcoin.org/en/
See also. Erik H. Nichola B. Supply Chain Finance And Blockchain Technology the Case for Reverse Securitization. Springer 2018

35 Ibid

36 "Bitcoin: A Peer-to-Peer Electronic Cash System."
Available at https://bitcoin.org/en/bitcoin-paper [accessed 9 February 2021]

37 Ibid, Pg. 1 Abstract.

The whole system is rooted in the rivalry between credit-based systems and cash-based systems in e-commerce. Cash based systems provide anonymity compared to the credit-based systems.

a) FirstVirtual, VISA, Mastercard and PayPal

In a credit-based system, the merchant required your data to be given to them before carrying out a transaction. That data included your bank details so that the merchant would be able to redeem their money. This was hard during the early days of the internet; in fact, it was considered unwise to hand over your credit card details to online vendors of unknown repute over an insecure channel. In such an environment, there was a lot of interest in the intermediary architecture.[38] An intermediary would work as such, the buyer would provide their credit card details to the intermediary who would then help in the purchase of the products – the intermediary and the merchant would then settle themselves at the end of the day.

A company called FirstVirtual was among the earliest founded intermediaries.[39] With FirstVirtual, the customers had to establish an account with FirstVirtual using a credit card. To make an online purchase, the customers sent their First Virtual ID number to the participating vendor, who in turn emailed First Virtual and the customer for confirmation. The money was then transferred to the vendor via the Automated Clearing House (ACH). However, VISA and Mastercard developed the SET architecture at the time.[40] In SET, to make a purchase, your browser would pass your view of the transaction details to a shopping application on your computer which, together with your credit card details would encrypt it in such a way that only the intermediary would decrypt it. Having encrypted your data in this way, you can send it to the seller knowing that it's secure. The seller blindly forwards the encrypted data to the intermediary — along with their own view of the transaction details. The

38 A. Narayanan et al, "Bitcoin and Cryptocurrency technologies" Feb 9, 2016

39 Information available at https://www.pcmag.com/encyclopedia/term/first-virtual [accessed 11 February 2021]

40 A. Narayanan et al, "Bitcoin and Cryptocurrency technologies" Feb 9, 2016

intermediary decrypts your data and approves the transaction only if your view matches the seller's view. This architecture was adopted by Cyber Cash[41] which apart from dealing in credit card payments also had virtual coins called Cyber Coins.[42] However Cyber cash and SET failed to work due to their requirement that each user had to acquire a certificate

b) Digi Cash, Hash Cash, Bi-money, Bitgold

In a cash-based system, the earliest ideas of cryptography to cash were from David Chaum in 1983. They were hinged on solving the issue of double spending and to keep the online system anonymous.

Digi Cash was started in 1989 to commercialise the ideas of David Chaum. This is one of the earliest companies to try and solve the issues with online payments.[43] So, let us say a person issues out pieces of paper saying that the bearer of one of those papers will redeem 1000 shillings when presented to that person with his signature. If people believe the promise will be kept and that the signature cannot be forged, they will pass around those papers as bank notes. However, if that was the case with digital notes, we would have a problem of double spending.[44] Hence, Digi Cash was a form of an electronic payment which required user software to withdraw notes from a bank and designate specific encrypted keys before it can be sent to a recipient. This advancement of public and private key cryptography allowed electronic

41 Founded in August 1994 by Daniel C. Lynch. More Information available at https://www.pcmag.com/encyclopedia/term/cybercash [accessed 11 February 2021]

42 This was a micropayment system — intended for small payments such as paying a few cents to read an online newspaper article.

43 Will Kenton, "Digi Cash." Available at https://www.investopedia.com/terms/d/digicash.asp Updated on December 19, 2020 [accessed 11 February 2021]

44 Investopedia definition by Jake Frankenfield. Double spending Is the risk that a digital currency can be spent twice. This is because digital information can be reproduced relatively easily by savvy individuals who understand the blockchain network and the computing power necessary to manipulate it. It is a unique risk for cryptocurrencies as physical currencies cannot be easily replicated, and the parties involved in a transaction can immediately verify the authenticity and past ownership of the physical currency. That is of course excluding matters involving cash transactions. Available at https://www.investopedia.com/terms/d/doublespending.asp [accessed 11 February 2021]

payments to become untraceable by the issuing bank. It also had a system of blind signatures through which security of its users was improved.[45] Therefore the clients were anonymous, so the bank could not trace their transactions, whereas the merchants were not anonymous since they had to return to the bank with coins as soon as they received them.

Digi Cash was the first to try and solve the problems of cash payments in e-commerce using cryptography, or at least it is among the first. But it had one problem – it was hard to persuade the merchants and the banks to adopt it. It also did not support user to user transaction but rather user to merchant transaction

Digi Cash was then followed by other ideas. To create a free-floating digital currency, one needs to create something scarce by design. This is what gives it real value. Scarcity is the reason as to why, gold has been used to back money for a long period.[46] The earliest company to solve this scarcity issue was Hash Cash.[47] This Hash Cash proof of work function has a complex mathematical understanding that is irrelevant for this paper. However, our pick is that bitcoin uses a similar computational puzzle as Hash cash with a few improvements.[48] Observe that in Hash cash, your cost to solve a number of puzzles is simply the sum of the individual costs, by design.

Another key element in the bitcoin system is the ledger system of record keeping. This is made possible through blockchain technology. This technology

---

46 Principles Of Economics. Chapter 27 Available at https://opentextbc.ca/principlesofeconomics/chapter/27-1-defining-money-by-its-functions/ [Accessed 12 February 2021]

47 The Hash Cash proof of work function was invented by Adam Buck in 1997. Available at https://en.bitcoin.it/wiki/Hashcash#History [Accessed 12 February 2021]

48 Extract from the Satoshi Nakamoto White Paper, "To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hash cash, rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash." Page 3. Available at https://bitcoin.org/en/bitcoin-paper [accessed 12 February 2021]

is quite old but it was first proposed by Haber and Stornetta.[49] Their scheme consisted of a proposal for a method of secure time stamping of digital documents not digital money. The goal of time stamping is to give an approximate idea of when a document came into existence and there is an order for these created documents.

Picking the above ideas, Bitcoin then combines the idea of using computational puzzles to regulate the creation of new currency units with the idea of a secure time stamping to record a ledger of transactions and prevent double spending.[50] There were earlier models like these way before Bitcoin – B-money[51] and Bitgold.[52] However, B-money and Bitgold were informal proposals Neither took off, nor was implemented directly.

Bitcoin has several important differences from b-money and Bitgold. In those proposals, computational puzzles are used directly to mint currency. Anyone can solve a puzzle and the solution is a unit of money itself. In Bitcoin, puzzle solutions themselves don't constitute money. They are used to secure the block chain, and only indirectly lead to minting money for a limited time. Second, b-money and Bitgold rely on timestamping services that sign off on the creation or transfer of money. Bitcoin, as we've seen, doesn't require trusted time stamping, and merely tries to preserve the relative order of blocks and transactions.

Combining all these features, Bitcoin would morph up into a sophisticated engine representative of consumer best interests as it is today.

- **Crypto currency Trust**

---

49 S. Haber, W. S. Stornetta. Secure Names For Bistrings. CCS 1997

50 An extract from the Satoshi Nakamoto White Paper, "We propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions." Pg.8 Available at https://bitcoin.org/en/bitcoin-paper [accessed 12 February 2021]

51 This was by Wei Dai in 1998.

52 This was by Nick Szabo – there is still confusion as to whether it was as early as 1998 or 2005

For any money form to work, that money form should be able to gain trust. Therefore, the concept of trust is essential for the adoption of any currency.[53] In the fiat model of currency, governing bodies create and sustain public trust through different regulations and a central authority, in Uganda's case, – Bank of Uganda.

Through the central authority, the governing authority through monetary policy will control the use of fiat money to avoid inflation and deflation, hence keeping the trust.

Some have argued that without trust, Cryptocurrencies would be worthless as they lack intrinsic value contrary to gold as it has intrinsic value.[54] There are two or more ways in which Cryptocurrencies have come to gain trust from the public. The first is through its own system[55] and the other is through the concept of Universal acceptance.

In order to achieve its goal of a peer-to-peer transaction, Cryptocurrencies replace the central authority – trusted third parties responsible for creation of trust with an electronic cash-based system that uses cryptographic proof instead of trust.[56] This is achieved through the inviolable decentralised block chain system. Trust is therefore created at a decentralised level unlike in the fiat currency model that is centralised.[57]

The other concept is that of universal acceptance. For some time now, most governments have opted to ban cryptocurrencies as they try to understand the technology deeper.[58] However, on the other hand we have seen big tech Multi-

---

53 Vigna and Casey, The Age of Cryptocurrency.

54 Check the value-based arguments on https://www.investopedia.com/ask/answers/100314/why-do-bitcoins-have-value.asp [Accessed 7 March 2021]

55 Venkata M. Bikesh U. et al "Understanding the creation of trust in cryptocurrencies: the case for bitcoin." Available at https://link.springer.com/article/10.1007/s12525-019-00392-5 [accessed 5 March, 2021]

56 An example is found in the Satoshi Nakamoto white paper.

57 https://boycewire.com/fiat-money-definition/ [accessed 6 March, 2021]

58 Some have even gone ahead to experiment their own state backed cryptocurrencies such as the Russian Crypto rubble.

national companies – Tesla[59], Facebook[60]. adopt the cryptocurrency mode of financial transaction such as accepting payment in Bitcoin. This has shifted the whole conversation regarding the trust of bitcoin.[61] While governments may not be interested in this technology, Technology enthusiastic companies have gone ahead to accept, support and invest in cryptocurrencies and this builds trust that is even beyond any borders as these companies do not have limited jurisdiction that the ancient monarchs had in order to create trust in a currency.

The replacement of trusted third parties without removing the concept of trust is key to why Bitcoin and other cryptocurrencies offer a viable and attractive alternative to the conventional model of government backed fiat.

- **Transactions under Cryptocurrencies**

a) Virtual Wallets

In order to have a complete set of anonymity to their users, the cryptocurrencies have a concept for a virtual wallet. A virtual wallet is a software with a digital address that allows access to the crypto currency's block chain for purchases, transfers and storage of the currency.[62] Virtual wallets are comprised of two hash outputs of 64-digit strings which make up the public key and secret key. The virtual wallet allows users' identities to considered pseudonymous, because buyers and sellers are only identified by their public wallet address; moreover, a user is not restrained to a single wallet. One may choose to create an unlimited number of wallets.

---

59 The company has already bought a large stock of Bitcoin and plans to accept it as a payment. Available at https://www.cnbc.com/2021/02/08/tesla-buys-1point5-billion-in-bitcoin.html [accessed 7 March 2021]

60 Facebook Co-founded the Libra project – a crypto currency that recently has changed its name from Libra to Diem. https://www.cnet.com/news/facebooks-controversial-cryptocurrency-gets-a-new-name-diem/ [Accessed 7 March 2021]

61 Read the effect of Tesla's purchase of bitcoin worth 1.5 billion on Bitcoin's stock and Trust on https://theconversation.com/bitcoin-why-a-wave-of-huge-companies-like-tesla-rushing-to-invest-could-derail-the-stock-market-154966 [accessed 7 March 2021]

62 Joseph J. Paul R. Blockchain A Practical Guide To Developing Business Law And Technology Solutions Mc Grow-Hill Education 2018 at pg. 18

The public key is the identity of the user whereas the secret key is the secret signature one uses to verify any transaction on the blockchain. The secret key is supposed to be unforgeable at least theoretically. The virtual wallet details – the public key and the secret key may be kept electronically on the internet, computer or on a piece of paper. However, loss of these two means that the coins one has on such a wallet are lost forever and so is the case when one accesses someone else's virtual wallet for malicious purposes.

It should be noted that one can create a new identity whenever they want on the cryptocurrency ecosystem. It is also noteworthy that since there is a record of every transaction ever made, the law enforcement agencies can track transactions between known public keys to partially break the anonymity of the system. I say partially because the real challenge comes with connecting those keys to real world addresses. This would be a whole easy problem to address in the classic fiat model where there are trusted third parties to track all transactions and who is behind all the accounts that would be in question.

b) Crypto Currency Exchanges

These exchanges work just like any other financial exchanges. They accept storage of cryptocurrencies and promise availability on demand just like banks. They also offer a platform for exchanging fiat currency with cryptocurrencies, however, subject to regulation. The plus side here is that they provide a connection between the Crypto currency economy and the flows of cryptocurrencies, with the fiat currency economy, so that it's easy to transfer value back and forth. If one wanted to exchange fiat to cryptocurrency, they would have to first register with the cryptocurrency exchange and then use a wire transfer or credit card or bank account to exchange.

However, such exchanges may be easily monitored and the major objective of anonymity would be compromised.

The discussion above by no means does cover the fully mathematical – technological and history of the functionality of the cryptocurrency however

gives an almost direct link to the functionality of cryptocurrencies and the potentially possibility of governments' control of the same. The next phase we will discuss the possible responses that states have to take or have taken to control cryptocurrencies and their different justifications.

3.0 POSSIBLE RESPONSES TO CRYPTOCURRENCIES BY SOVEREIGN STATES

With the ever-increasing popularity of cryptocurrencies as an alternative and unregulated form of transaction, there are three ways in which a sovereign state can respond - total ban, regulation or adoption of cryptocurrencies. A state may opt for one of the mentioned or can actually use any two of the mentioned. Uganda's response has been through the central bank, and the legislators are still quiet despite its growing popularity. This section will discuss the different responses and the rationale as such.

3.1 Ban/Prohibition Of Cryptocurrencies.

Most states' first response has been to totally ban/prohibit cryptocurrencies. States have to exercise control on cryptocurrencies in order to maintain their legitimacy. Therefore, a legislation or two are passed to target cryptocurrency users, designers or the cryptocurrencies themselves. Prohibition of cryptocurrencies happens for various reasons, inter alia, to reduce criminality, to protect civil rights of citizens, avoid weakening of the state's ability to control capital flow of wealth, to prepare for the release of a state backed cryptocurrency.[63]

While we consider other legitimate reasons to ban cryptocurrency, preparation for a state backed cryptocurrency seems to be the profound reason for most states. The justification is profoundly attractive – there cannot be a total ban

63 Ryan L. Frebowitz, "Crypto Currency and State Sovereignty." Thesis. Naval Post Graduate School. Monterey, California. June, 2018 pg. 38

on crypto currency as most people that can access the internet can make transactions[64] unless the state can be able to shut down the internet for its citizens. This obviously is understandably not a very wise decision for any sovereign state. But for the reasons expounded on below banning stateless cryptocurrencies is justifiable.

a) State Backed cryptocurrency

Introduction of a state backed cryptocurrency is one reason why most state's first response is to ban stateless cryptocurrencies. The question is whether it's possible for a developing country to introduce a state backed cryptocurrency and whether it's justifiable.

The state backed cryptocurrency however has to look different from these other stateless cryptocurrencies in as far as having a central figure is concerned – they are centralised rather than decentralised with a controlling entity such as the national bank.

b) Increase state's capital controls

Cryptocurrencies have the ability to transact seamlessly across sovereign state's borders.[65] For states that are in an economic crisis, bypassing the capital controls can be disastrous as the economy may not be stabilised easily. Capital controls are rules or regulations that are put in place to limit the flow of income in and out of the country. Through avoiding the fees, taxes and tariffs that are associated with traditional fiat currency, cryptocurrency transactions are much cheaper for both transacting parties hence their possibility of preference.

For a state to keep its legitimacy hence sovereignty, banning stateless cryptocurrencies to increase its capital controls and avoid Capital flight[66] is

64 A. Narayanan et al, "Bitcoin and Cryptocurrency technologies" Feb 9, 2016
65 Supra FN 10 pg. 39
66 According to Investopedia, "Capital flight is a large-scale exodus of financial assets and

justifiable. Through legislation to ban cryptocurrencies states make exchange of fiat currency to cryptocurrency difficult hence complicating the process by which wealth is exported outside the nation.

3.1.1 Difficulties Associated with Ban or Prohibition of Cryptocurrencies.

So far, most states have opted for prohibition of cryptocurrencies – Uganda inclusive.[67] The question as to whether this is the best response is up for discussion as we evaluate its drawbacks. Regardless of the reason to ban or to partially ban, the end goal is to discourage the use of the cryptocurrencies. This eventually cripples innovation in itself and encourages illicit use of the crypto currencies as they have been widely accepted and popular.[68] Cryptocurrencies can easily be accessible by anyone with access to the internet either with a phone or a computer.[69]

For a ban or prohibition to be successful, it has to cause the essential shutdown of the internet. This, of course, may cause a civil uprising which would inevitably question the legitimacy of the government. For a government to ban cryptocurrencies, it must demonstrate the means to disrupt their domestic use, if it is to be successful. The size of the state needed and the punishments for these law breakers matter a great deal in order for the policies to work.[70] A total ban would in our view, be one that would pose difficult challenges both to the enforcers of the ban and to the essential growth of the innovation sector as far as cryptocurrencies are concerned.

---

capital from a nation due to events such as political or economic instability, currency devaluation or the imposition of capital controls." Elvis Picardo, "Capital Flight," Investopedia, January 5, 2004, https://www.investopedia.com/terms/c/capitalflight.asp also see "Capital Flight," Investopedia, https://www.investopedia.com/terms/c/capitalflight.asp#ixzz5Czwv8Th0 [accessed 15 October 2020]

67 Supra FN 3

68 Maria Demertzis & Guntram B. Wolf, "The economic potential and risks of crypto assets: is a regulatory framework needed?" Policy Contribution Issue n°14 | September 2018.

69 Global Legal Insights. Blockchain and Cryptocurrency Regulation. 2019 1st Edition.

70 Joshua Hendrickson and William Luther, "Banning Bitcoin," Journal of Economic Behaviour & Organization 141 (September 2017): 194.

3.2.0 Adoption Of Cryptocurrencies.

Previously, we looked at the rationale for prohibition of cryptocurrencies and one was to pave way for a state backed cryptocurrency. There are two ways through which a state can adopt crypto currencies – Recognition of prior existing stateless cryptocurrencies as legal tender and Introduction of a state backed cryptocurrency as legal tender.[71] There are various reasons for adoption of cryptocurrencies inter alia – to bypass sanctions, cheaper transaction costs but for the benefit of this paper two reasons are discussed.

a) To Incorporate the Unbanked

Theoretically, less developed countries like Uganda may opt for cryptocurrencies to incorporate the unbanked. The unbanked are those that cannot access banking services such as store or secure money in banks and can neither make purchases online nor transact outside their locality. With a state backed cryptocurrency by the central bank then the said cryptocurrency will cover this unbanked part of the population hence allowing them access to the state financial structure. There are a number of reasons for the existence of the unbanked, inter alia, lack of adequate access to and banking infrastructure, weak institutional identification process that makes investment in banking risky and unlikely. Therefore, making them a potential untapped potential market for goods and services.

Reference for this can be traced to the mobile money use in Uganda. The people that transact using mobile money Vis a vis those that use banks. There is a huge number of people that do fall in this category of the unbanked.

b) The Auditability of Cryptocurrencies

States can benefit much more from cryptocurrencies than anticipated when they first arrived. A state backed cryptocurrency has the ability to maintain every transaction through the ledger technology, centralised or decentralised.

---

71 Supra FN 10 pg. 69

This will go far in auditing and enhancing Anti Money Laundering laws. This will, as well, be able to provide the legal evidence needed against the corruption and embezzlement of funds as these are easily trackable. The state backed cryptocurrency would also incentivise the users to register and transact peer to peer basis than other electronic methods of transaction, and in any case, a licit user of the currency would have no trouble with registration. Another added advantage is that a state backed cryptocurrency would theoretically encourage legal employment of the currency as against illegal employment of the other stateless cryptocurrency.

3.2.1 Difficulties Associated with Adoption of Crypto currencies

With adoption of cryptocurrencies, there is an assumption that every citizen has access to the internet in a working economy. This poses a great challenge to the adoption strategy. Internet coverage, for instance in Uganda, is about 48%.[72] There are various challenges that come with adoption of cryptocurrencies. Chief among them, and a concern for this paper, is the speculative attack, the domestic pushback and the domestic institutional pushback.[73]

A speculative attack on a currency occurs when an investor wishes to take advantage of a 'weak currency,' a currency that has depreciated in value relative to other currencies.[74] The objective of a speculative attack is to take advantage of the maturity mismatch of funds. This is a term used to describe a discrepancy when a bank is forced to buy a weaker currency at a loss. This eventually depletes the bank's supply of the weaker currency overtime thereby

---

72 It is estimated that internet penetration in Uganda is at only 48% (42% of Uganda's Population Now Connected to Internet https://www.newvision.co.ug) [accessed 13 March 2021]

73 Supra FN 10.

74 Plassaras describes the speculative attack, writing "the attack begins by taking what is known as a 'short position' in the currency. To do this, the attacker borrows a sum of the weak currency and sells it for a stronger (more valuable) currency, with the intention of buying the weak currency back for less than the attacker sold it for. If the currency continues to depreciate in value after the short sale, the attacker makes a profit when they buy it back." Plassaras, "Regulating Digital Currencies.

destabilizing the foreign currency exchange market. A solution to this would be for the IMF to hold a reserve stock of the cryptocurrency so as to get the affected state out of the danger.

Adoption of the cryptocurrency presents hurdles both in implementation and adoption. This is because the said currency may face a domestic pushback. Citizens may refuse to adopt the cryptocurrency due to its complexity over physical money that can be held.

3.3 REGULATION OF CRYPTOCURRENCIES

There are various justifications for the regulation of cryptocurrencies, however, the paper focuses on – consumer protection and protecting the monetary policy. For if the government loses these then there is loss of legitimacy and sovereignty. As of the writing of this article, there is no country that has issued out regulations for cryptocurrencies on a supranational level.

This has been largely because it is difficult to find a regulation that may not necessarily affect the rights of the citizens to own and transact in cryptocurrencies and at the same time keep the state's needs. Cryptocurrencies are also hard to define thereby hard to regulate. However, this paper proposes a new approach of regulation later that is elastic and progressive enough to make regulation much easier.

a) Consumer and Investor protection

The digital nature of cryptocurrencies makes them accessible to the general public provided that public is digitally aware. Broad access is obviously desirable, but exposes vulnerable groups. In a regular financial world such investments like Initial Coin Offerings should be done by venture capitalists who understand the risks.

However, beyond the risks, there have been possibilities of fraud in situations where the system has been beaten. For example, a group of hackers known as the "51 crew" took control of more than 51% of two blockchain clones shift and

krypton thereby defrauding close to $65 million in bitcoin through taking over the verification process.[75] Such cases of fraud and uncertainty in the cryptocurrency world, therefore, call for policy framework on this fast-changing technology. The issues of consumer and investor protection need to be seriously considered.

b) Protection of monetary policy

This is undeniably a very essential creature of the legitimacy of any government. With the wide acceptance and use of a stateless cryptocurrency in a sovereign state, the citizens will eventually bypass the state and the central bank completely if there is no regulation. We need take consideration that cryptocurrencies may take a high rise in Uganda in the next decade or so and as such regulation to protect the monetary policy is needed to avoid the significant drawbacks, once ignored

3.3.1 Difficulties Associated with Regulation of Cryptocurrencies.

Regulation of a destructive technology is, in itself, unrealistic and unattainable, as a result of the principle of technology neutrality.[76] Technology changes exponentially while regulation changes incrementally hence regulation often lags behind innovation. Regulation could hamper or prevent innovation.[77] Therefore regulation of cryptocurrencies should be approached with caution. The fundamentalists and crypto anarchists believe entirely in a system that is away from third party regulators and would eventually develop a more complex one to avoid the regulation. On the other hand, it is the tendency of the technology to evolve that is crucial in justifying regulation.

---

75 See: https://www.huffingtonpost.in/raja-raman/blockchain-can-transform-the-world-but-is-it-foolproof_a_21660586/ [accessed 17 March 2021]

76 Joseph F. Borg & Tessa Schembri," The regulation of blockchain technology" GLI – Blockchain & Cryptocurrency Regulation 2019, First Edition. Global Legal Group Ltd, London.

77 Supra FN 15.

Therefore, there is need to strike a balance between an appropriate level of regulation that minimally infringes on the citizen's rights to own and use cryptocurrencies and a level of control on cryptocurrencies meeting the sovereign state's needs.[78] With regulation, there is a need to define and classify cryptocurrencies. The needs of individual states vary and are dependent upon the political, economic, and law enforcement requirements – a challenge to the sovereign state.

4.0 THE CASE FOR UGANDA – RECOMMENDATIONS

Having gone through the different ways in which the state can respond to the quickly emerging technologies, there is need to evaluate the best response for the state of Uganda. This will be affected by different factors, political and socioeconomical.

For any state sovereignty to survive this technological innovation, two things must be taken into consideration – the state's monetary policy protection[79] and protection of its citizenry financial investment and consumerism. Therefore, with reference to the justification for a regulatory response discussed earlier – the recommendations will generally be of a regulatory nature, side-lining the ban and adoption with reasons given.

In order to carry on a ban on cryptocurrencies, enforcement would be impracticable as it would literally require shutting down the internet. One of the justifications for a ban is to prepare the cryptocurrency space for a state backed cryptocurrency. This ideally would not be a preferrable agenda for a 3rd world economy[80] like Uganda's.

---

78 Supra FN 10.

79 Available at https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwj4y5OnsZ7vAhVjqnEKHQ7BBGsQFjAAegQIARAD&url=https%3A%2F%2Fwww.imf.org%2Fexternal%2Fpubs%2Fnft%2F2006%2Fcdmf%2Fch1law.pdf&usg=AOvVaw0yy6O6aHX1GF7Si0Kw29YF [accessed March 2021]

80 Uganda has a 3rd world economy. Check data available at https://theconversation.com/whats-needed-to-take-africa-from-third-to-first-world-in-25-years-61418 [accessed 6 March 2021.]

For any country to adopt cryptocurrencies, there is a need for its citizenry to be capacitated to adopt the technology. There would be a need for every citizen to access internet cheaply, access a smart phone and a computer. This is not feasible in a country like Uganda. Internet usage and penetration in Uganda still remains at 48%,[81]his clearly does not favour the adoption of the technology unless that challenge is to be addressed which might take a long time.

- **Creation of a broad legal regime concerning Cryptocurrencies.**

The government, through its legislative arm, should create a broad regulation to regulate cryptocurrencies. Currently the Ugandan government does not recognize any crypto-currency as legal tender in Uganda.

The government of Uganda has not licensed any organization in Uganda to sell crypto-currencies or to facilitate the trade in crypto-currencies and so these organizations are not regulated by the Government or any of its agencies. As such, unlike other owners of financial assets who are protected by Government regulation, holders of crypto-currencies in Uganda do not enjoy any consumer protection should they lose the value assigned to their holdings of crypto-currencies, or should organization facilitating the use, holding or trading of crypto-currencies fail for whatever reason to deliver the services or value they have promised.[82]

However, it pays more if the regulators opted for a more open-minded stand as it's clear that cryptocurrencies have certain indelible features that can transform financing forever and in order to make a regulation, certain terms need to be considered.

a) Redefine Cryptocurrencies.

---

81 Data provided by Data Reportal accessible at https://datareportal.com/reports/digital-2020-uganda [accessed 7 March 2021.]

82 Public Statement On Crypto Currencies By The Minister Of Finance. Dated Tuesday October 1st 2019. Available at https://www.finance.go.ug/press/public-statement-cryto-currencies-minister-finance [accessed 17 March 2021]

This is to avoid the absurdity that would be created while interpreting the regulation due to uncertainties. Take an example in what happened in *US v Ulbricht.*[83] This case involved a website that was used to sell illegal drugs and payment was wired through cryptocurrency. There was a huge contention on whether cryptocurrencies were property or money. The defendant was acquitted because the law only construed cryptocurrency as property and not money.

It is our view that cryptocurrency is a revolutionary new step forward in innovative, open-source technology, and unless laws drastically change to regulate cryptocurrencies, companies and businesses are likely to continue refining blockchain technology well into the future. Therefore, rather than allowing individual regulatory bodies to interpret cryptocurrency under their jurisdictions, the creation of an all-encompassing categorization for virtual currencies with clearly distinct and subordinate legislation, specifically distinguishing licit and illicit cryptocurrency actions, would prevent confusion regarding cryptocurrencies among citizens and businesses.

Take a case of the State of Alabama.[84] The state of Alabama enacted The Alabama Monetary Transmission Act, effective August 2017. The act defines "monetary value" as "[a] medium of exchange, including virtual or fiat currencies, whether or not redeemable in money." Notably, Alabama's Securities Commission has emerged as one of the most active agencies to address fraud in the cryptocurrency industry.[85] The Alaskan bill of 2017 defines cryptocurrencies to cover "digital units of exchange that have a centralized repository" as well as "decentralized, distributive, open-source, math-based, peer-to-peer virtual currency with no central administrating

---

83 The case is available at https://casetext.com/case/united-states-v-ulbricht-13 [accessed 6 January 2021]

85 See https://www.coindesk.com/alabama-the-unlikely-frontline-for-americas-crypto-fraud-crackdown. [accessed 13 March 2021]

authority and no central monitoring or oversight."[86] Colorado through the Colorado Digital Token Act defines a Digital Token as a digital unit with specified characteristics, secured through a decentralized ledger or database, exchangeable for goods or services, and capable of being traded or transferred between persons without an intermediary or custodian of value.[87] These are but a few definitions by different jurisdictions that can shape what our definitions can be.

Through such a legislation with a broader definition of cryptocurrencies, we will have gone as far as covering the technology that has not yet arrived but is on our door steps. The Ugandan legislature, therefore, needs to enact a law that clearly defines or redefines cryptocurrencies in a broader manner in order to avoid absurdity caused by the uncertainty nature of this technology.

b) Regulation of specific entities

A regulation of some specific stake holders is needed. These entities may include Cryptocurrency exchanges. Such a regulation may go as far as targeting the privately owned financial institutions functioning as key parts of a cryptocurrency network. Examples of what such a regulation may entail would be the creation of minimum consumer protection requirements to which the exchange or other institution would be subject or the requirement of locally owned exchanges to keep and provide records to regulatory bodies when necessary.

c) Acceptance of cryptocurrencies to work alongside the existing Financial Framework

While we think about regulation, we may also consider opening the existing financial space to accommodate cryptocurrencies. One justification even

86 H.B. 180, 30th Leg., 1st Sess. (Alaska 2017)
87 see https://leg.colorado.gov/bills/sb19-023. [accessed 13 March 2021]

though unexplored is that the auditability of cryptocurrencies is both ideally and practically attractive especially for a country that is faced with a scourge of embezzlement and corruption[88] since there is evidence of every transaction. The technology will also supplement on the existing financial Frame work.

However, this will work through the following.

I. Creation of an Information and Moral suasion policy.

Cryptocurrencies, as earlier discussed, gain their trust through universal acceptance. Regulation will hardly work if cryptocurrencies are accepted but the people are unaware of what they are. The main objective for this policy is to protect consumers and investors in this new technological space through universal awareness. Uganda has not been spared as far as defrauding consumers and investors is concerned.[89] This is because the digital nature of crypto assets makes them directly accessible to the general public, provided people are digitally aware.

Broad access is desirable, but also exposes vulnerable groups. In a regular financial world such investments like Initial Coin Offerings should be done by venture capitalists who understand the risks. Elsewhere this technology has picked the interest of youths and entrepreneurs that seek to use it in various opportunities – to some it is an investment whereas to others, it is a medium of exchange that may come good for evading taxes.[90] Uganda's population has a

88 Check https://www.ganintegrity.com/portal/country-profiles/uganda/ [accessed 7 March 2021]

89 Dozens Count Losses in Sham Cryptocurrency Scheme, Daily monitor;5/12/19 available at https://www.monitor.co.ug/uganda/news/national/dozens-count-losses-in-sham-cryptocurrency-scheme-1863024

90 For example, the March 2018 US Student Loan Report quotes the results of a survey, in which about a fifth of all participating students had used financial aid money to invest in cryptocurrencies, like bitcoin. Also available at https://studentloans.net/financial-aid-funding-cryptocurrency-investments/ [accessed 6 March 2021]

tendency of accommodating any technological business that makes it easier to work – take an example on how quickly sports betting arose.[91]

Without regulation there is no remedy for the thousands that may fall prey for this technology where fraud happens. This would be absurd for a country that may not guarantee consumer and investor protection hence losing legitimacy.

5.0 CONCLUSION

There is cause to believe that the emerging crypto sector has a bearing on the dramatic events worldwide not only in virtual currencies but e-commerce as a whole. Increasingly, physical space is becoming a concept of gone days.[92] And as such, the debate on devising a mechanism to oversee but also set a minimum standard is a much needed one.

We are looking at a still young technology that is evolving alongside the demand for it. The technology's future use is still unclear as is its place in the financial eco system. The unique investment characteristics and unfamiliar metrics make it impossible to apply traditional valuation mechanisms and techniques. Thus, the opinions given in this paper may even be obsolete by the near future but in any case, we should not wait for the worst to happen for us to start having discussions about this young but rapidly evolving technology.

Most states have not issued any regulations regarding to cryptocurrencies. Some states have issued guidance, opinion letters, or other information from their financial regulatory agencies regarding whether cryptocurrencies are "money" under existing state rules, while others have enacted piecemeal

---

91 Reagan W, Sports Betting and Gaming; Our youths are losing out. Available at https://parliamentwatch.ug/sports-betting-and-gaming-our-youth-are-losing-out/ Published 6 years ago. [accessed 6 March 2021]

92 Airbnb for instance which is an online platform where property owners and visitors to over 100 countries agree on short term contracts generates over $1 billion annually without owning a single physical premise

legislation amending existing definitions, to either specifically include or exclude digital currencies from the definition.

Uganda itself has issued out statements through the Ministry of Finance and Bank of Uganda to state that cryptocurrency use should be done with caution a there is no consumer protection or any other protection. The authors of this paper are hopeful that over the next few years Uganda will craft a regulation that balances the dual needs of protecting consumers and investors from businesses operating in the fledgling industry while also promoting continued innovation by not saddling cryptocurrency businesses with regulatory burdens that make it financially impractical to operate as it will be once acceptance becomes futile. Whether we like it or not Cryptocurrencies are a revolutionary currency structure that are here to stay. In order for the Government of Uganda to keep its legitimacy and the state sovereignty, they ought to first acknowledge this technology, and then provide an avenue in which the technology will be used in our financial space.

LIST OF REFERENCES

1) A. Narayanan et al, "Bitcoin and Cryptocurrency technologies" Feb 9, 2016
2) Bank of Uganda. Warning to General Public about "One Coin Digital Money" operations in Uganda. Feb 14, 2017 http://www.bou.or.ug/bou/bou-downloads/press releases/2017/Feb/Bank-of-Uganda-warning-on-One-Coin-Digital-Money-in-Uganda-pdf
3) Corporate Finance Institute, "What is Fiat Money?" Available at https://corporatefinanceinstitute.com/resources/knowledge/economics/fiat-money-currency/
4) Erik H. Nichola B. Supply Chain Finance And Blockchain Technology the Case for Reverse Securitization. Springer 2018
5) Global Legal Insights. Blockchain and Cryptocurrency Regulation. 2019 1st Edition.
6) Hyman P. Minsky, The Financial Instability Hypothesis: An Interpretation of Keynes and an Alternative to "Standard" Theory, in Can "It" Happen Again? Essays On Instability And Finance 59 (1982) (originally published in 1977 on the tendencies of a financial system to destabilize endogenously).
7) Introducing Money available at https://courses.lumenlearning.com/boundlesseconomics/chapter/introducing-money/
8) James R Crawford. Brownlie's Principles Of Public International Law. 8th Edition.
9) Jason Hall, "Fiat Currency. What it is and Why it's Better than a Gold Standard." The Motley Fool. Available at https://www.fool.com/investing/general/2015/12/06/fiat-currency-what-it-is-and-why-its-better-than-a.aspx

10) Joseph F. Borg & Tessa Schembri," The regulation of blockchain technology" GLI – Blockchain & Cryptocurrency Regulation 2019, First Edition. Global Legal Group Ltd, London.

11) Joseph J. Paul R. Blockchain. A Practical Guide To Developing Business, Law And Technology Solutions. Mcgraw-Hill Education 2018 1st Edition

12) Joshua H. and William L. "Banning Bitcoin," Journal of Economic Behaviour & Organization 141 (September 2017): 194.

13) Karin P. "Monetary Practices and Currency Transition in early colonial Uganda." The African Economic History Network. 18th July, 2016 Available at https://www.aehnetwork.org/blog/monetary-practices-and-currency-transitions-in-early-colonial-uganda/

14) Katharina Pistor, From Territorial to Monetary Sovereignty, Theoretical Inquiries In Law, Vol. 18, P. 491, 2017; Columbia Law School Center For Law & Economic Studies Working Paper No. 591 (2017). Available at "From Territorial to Monetary Sovereignty" by Katharina Pistor (columbia.edu)

15) Maria D, Guntram B. W. "The Economic Potential and Risks of Crypto Assets: Is a Regulatory Framework Needed? Policy Contribution. Issue No. 14| September 2018.

16) Maria D. & Guntram B. W., "The economic potential and risks of crypto assets: is a regulatory framework needed?" Policy Contribution Issue n°14 | September 2018.

17) Mathias D and Martin S," Money as a Unit of Account." Econometrica Vol. 85 No.5 2017 Available at https://www.jstor.org/stable/44955172?seq=1

18) Principles Of Economics, Chapter 27 – Defining Money by its functions. Available at https://opentextbc.ca/principlesofeconomics/chapter/27-1-defining-money-by-its-functions/

19) Public Statement On Crypto Currencies By The Minister Of Finance. Dated Tuesday October 1st 2019. Available at

https://www.finance.go.ug/press/public-statement-cryto-currencies-minister-finance

20) Reagan W, Sports Betting and Gaming; Our youths are losing out. Available at https://parliamentwatch.ug/sports-betting-and-gaming-our-youth-are-losing-out/

21) Robert A. Mundell, "Money and the sovereignty of the state." Columbia University.

22) Ryan L. F. "Crypto Currency and State Sovereignty." Thesis. Naval Post Graduate School. Monterey, California. June

23) S. Haber, W. S. Stornetta. SECURE NAMES FOR BISTRINGS. CCS 1997

24) Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (White Paper, Bitcoin 2008). 1 http://bitcoin.org/bitcoin.pdf

25) Venkata M. Bikesh U. et al "Understanding the creation of trust in cryptocurrencies: the case for bitcoin." Available at https://link.springer.com/article/10.1007/s12525-019-00392-5

26) Vigna and Casey, The Age of Cryptocurrency.

27) When Two Cowrie Shells Could Buy a Woman? The East African Magazine. Available at https://www.theeastafrican.co.ke/tea/magazine/when-two-cowrie-shells-could-buy-a-woman-1293988

28) Will Kenton, "Digi Cash." Available at https://www.investopedia.com/terms/d/digicash.asp Updated on December 19, 2020

29) Yaya F," The New Frontier in Terror Fundraising; Bitcoin." The Cypher Brief(blog) August 24, 2016.

30) Yuval N. H. MONEY. Vintage Minis.