Covenant University Journal of Politics & International Affairs, Vol.12 No. 1, June, 2024
ISSN: p. 2354-3558 e. 2354-3493 DOI: xxxxxxxxxxxxxx

Open Access Journal Available Online

Taming the Wind: Cryptocurrency, International Law, and Nigeria's National Security

[1]Abiola A. ISIKALU,
[2]Goodnews OSAH
[3]Uzzibi IRMIYA
[4]Temitope E. OMOSEBI

[1,2,3,4] Department of Political Science and Public Administration
Babcock University
Corresponding email: osahg@babcock.edu.ng

Abstract: This study aimed at exploring how international law can be extended to the cryptocurrency space and the plausible effects that this may have on the national security of Nigeria by reviewing relevant sources of information. The research questions that were addressed in this paper included: "In what ways can international law be used to regulate the cryptocurrency market?" and "How will such regulations impact national security in Nigeria?" The study found that Nigeria presents a case where cryptocurrency was banned and yet, its adoption has been increasing and its prohibition has worsened its use for illegal activities that threaten national security and economic health. Individuals and organisations have found ways to trade and own cryptocurrencies in the country without getting detected by relevant authorities in the country. By implication, Nigeria needs to re-consider its stance on cryptocurrency regulation. Most importantly, the development of an international regulatory framework that facilitates the successful extension of international law to the regulation of cryptocurrency can help Nigeria to improve its national security by tackling terrorist and other crime funding and tackling the use of cryptocurrency for corrupt practices such as money laundering and tax evasion.

Keywords: Blockchain-enabled technologies, Cryptocurrency, Decentralisation, National security, Nigeria, Terrorism, User autonomy

Introduction

According to Mukhopadhyay et al., (2016), cryptocurrency functions on a peer-to-peer digital and decentralised exchange system where cryptography is employed to generate and distribute digital currency units. Liu and Tsyvinski (2020) describe cryptocurrency as a digital financial system that serves as an alternative to traditional banks and is based on a technology – the blockchain –

that is yet to be fully understood. Cryptocurrencies provide users with an alternative financial system that is characterised by decentration, transparency in the processes of transaction, and users' total control of the management of their assets; and all these qualities of cryptocurrencies are facilitated by the blockchain technology (Miraz & Ali, 2018; Temi, 2022).

The adoption of cryptocurrency has been seeing a steady growth, albeit challenged by security concerns and antagonising policies, since its inception in 2008 with the first cryptocurrency – Bitcoin (Al-Amiri, Zakaria, Habbal, & Hassan, 2019). In recent years, higher adoption and transaction volumes are being recorded due to the increase in the public's knowledge about blockchain and cryptocurrency and due to the introduction of cryptocurrency-related innovations such as non-fungible tokens (NFTs), Web3.0, and the Metaverse (Ante, 2022; Akkus, Gursoy, Dogan, & Demir, 2022). According to de Best (2022) in a report for Statista, the 24-hour trade volume in the cryptocurrency landscape has gone as high as 500 billion U.S Dollars. Hence, the cryptocurrency landscape is a significant economic and social aspect that needs to be accorded adequate policy and legislative attentions. However, the central nature and the selling points of cryptocurrencies – decentralisation and user autonomy – make it highly difficult to provide and implement legislative actions in the cryptocurrency landscape. According to Politou et al., (2021), decentralisation refers to the distribution of the processes of transacting cryptocurrencies and other related activities across multiple servers; and it also refers to the concept of zero governance, that is, cryptocurrency, its ownership, and transactions are not controlled by any central regulatory authority. Decentralisation facilitates optimal security, fast transaction, and transparency in cryptocurrency systems (Anthony, 2021). The implication of zero-governance characteristics of decentralisation in cryptocurrency is that government institutions have limited ability to enforce any form of control or authority on cryptocurrency operations. Unlike in the case of traditional banks where apex regulators or the government can seize the asset of individuals due to suspicious transactions or illegal activities, governments do not have the ability to seize or control the cryptocurrency assets of an individual except the individual wilfully relinquishes their means of accessing the assets.

While cryptocurrency provides alternative financial systems, it has also facilitated diverse financial corruption and digital fraud. According to Sanz-Bas et al., (2021), individuals and criminal organisations leverage cryptocurrency to facilitate illegal financial transactions that remain untraceable, even out of the reach of the government. Using Spain as an instance, it is expressed that cryptocurrency systems have been adopted as hideout strategies for money laundering, financial sanction evasion, fraud, and other illegal financial activities (Sanz-Bas, del Rosal, Alonso, & Fernandez, 2021). In Nigeria, cryptocurrency systems have been used for terrorism and other criminal activity funding (Premium Times, 2022). Ozili (2022) reports that the Nigerian government made the decision to ban cryptocurrency because of the fraud and illegal financial activities that were associated with it in the country.

Considering the illegal activities that are perpetrated through cryptocurrency systems, different regions of the world are developing their legislative

frameworks for governing cryptocurrencies but, more importantly, there is a growing discourse on developing an international law for governing cryptocurrency markets. The World Economic Forum (2021) avers that legislative input from international bodies on the regulations of cryptocurrency are important because they influence regulations in countries and provide frameworks for addressing international cryptocurrency-related disputes. Narain and Moretti (2022) further assert that developing regulatory bodies for cryptocurrency, at an international level, will improve the safety of transactions and innovations in the space.

Questions on the best approach to develop international law for cryptocurrency regulations and the enforceability of the laws, however, persist in literature. In Guillaume (2019), it is expressed that the ability of private international law to contend with legal relationships that are formalised via the internet, especially via a decentralised infrastructure such as cryptocurrency, is highly debatable. This makes it key to comprehensively examine the nature of cryptocurrency and how the wings of international law can be extended to its regulation in an enforceable manner. It is also necessary to examine the plausible effects of international law regulations for cryptocurrency on specific countries. In this vein, the current paper is aimed at exploring how international law can be extended to the cryptocurrency space and the plausible effects that this may have on the national security of Nigeria by reviewing relevant sources of information. The research questions that will be addressed in this paper are.

1. In what ways can international law be used to regulate the cryptocurrency market?
2. How will such regulations impact national security in Nigeria?

2. Review of Literature

The consideration of cryptocurrency within the provisions of law has been addressed in literature to be complicated, especially on issues that are related to international resolution. According to Munoz (2020), there has been limited investigation into the applicability of international law to blockchain-enabled technologies such as cryptocurrency, and this is mostly because cryptocurrency disputes or its general nature appears to be non-addressable by the law. Further understanding is availed into the assertions by Munoz (2020) in Guillaume and Riva (2022). The authors introduced their argument on the difficulty of applying international law to cryptocurrency by making a case of how dispute resolution by means of classic arbitration is rarely considered in e-commerce disputes mainly because of the disparities in the legal provisions for disputes and consumer rights in different national regions. In the case of cryptocurrency transactions where parties are mostly anonymous and there are hardly traces of national origins, there are diverse complications in the application of international law to control the use of cryptocurrency and to address issues that ensue from its transaction such as disputes, breaches of agreement and crime funding (Guillaume & Riva, 2022). From the discussions above, it is seen that scholars identify the extension of international law to cryptocurrency as highly problematic. A central idea that is shared among the consulted studies is that the decentralised nature of cryptocurrency challenges the traditional approach to employing legal interventions. The decentralised nature of cryptocurrency arises from its reliance on

the blockchain technology which functions by distributing its nodes and operations across multiple servers and, as such, blockchain is referred to as a distributed ledger technology (DLT) (Munoz, 2020). Guillaume and Riva (2022) particularly reflect on a concept in cryptocurrency and blockchain-enabled platforms that is called 'decentralised autonomous organisations' (DAO). DAO is a form of governance in blockchain-enabled platforms which means that users have full control over their activities and platforms cannot make any authoritative decisions on users' assets or accounts (Guillaume & Riva, 2022; El Faqir, Arroyo, & Hassan, 2020). The nature of this governing style in cryptocurrency platforms invariably limits the extent to which laws can be enforced on the platforms.

Guillaume (2019) identifies cryptocurrency systems as payment systems and draws a comparison between them and payment systems that are built on regulated banking networks such as PayPal, Western Union, and credit card companies. It is noted that cryptocurrency networks are not regulated by central authority as done with systems such as PayPal and Western Union, which calls into question the enforceability of international law within the context of cryptocurrency systems. Furthermore, Guillaume (2019) considers cryptocurrency within the framework of private international law. The author moves from noting that cryptocurrency transactions have a legal scope as they suggest agreement between involved parties, to discussing that international private laws function by deploying the most relevant state-level private laws; and this "method does not appear appropriate, insofar as the Internet - like the blockchain - is an inherently intangible and transnational phenomenon" (Guillame, 2019, p. 61). Hence, the problem in identifying the regional sources of cryptocurrency transactions remains a challenge in the extension of international (private) law to cryptocurrency systems.

The lack of uniformity in national approaches to regulation of cryptocurrency assets and systems as identified is expressed in Narain and Moretti (2022), in a report for the International Monetary Fund. The authors argue that the issue in the regulation of cryptocurrency assets is not that there has been a lack of provisions for regulatory laws and policies, but that different state authorities have employed contrasting approaches which may be difficult to harmonise when international law needs to be enforced. A common dichotomy in the regulatory framework for cryptocurrency across nations is that some ban its usage while some promote its use and encourage cryptocurrency brands to open business outlets in their jurisdictions (Narain & Moretti, 2022). For instance, the Nigerian government took an opposition stance to the use of cryptocurrency by proclaiming a ban on cryptocurrency transactions in 2021 yet, this has not stopped Nigerians from owning cryptocurrency assets – in fact, the volume of cryptocurrency transactions in Nigeria has been soaring since the ban (Smith, 2022). Hence, it may be challenging to address conflicts in a cryptocurrency transaction between a brand from Nigeria and a brand from Japan where the use of cryptocurrency platforms is supported by the government (NotaBene, 2022).

Razon (2019) provides a critical attempt to the application of international law to blockchain-enabled systems. The author argues for the use of the General Agreement on Trade in Services (GATS) – a treaty by the World Trade

Organisation that was adopted in 1995 – to regulate international blockchain transactions including cryptocurrency. Razon (2019) asserts the need to first conceptualise blockchain and the systems that rely on it as "services" and not goods for the treaty to be applicable. In theory, the application of GATS to blockchain will enable a uniform approach to the application of international law to cryptocurrency activities and transactions/agreements.

The application of GATS provides a viable framework for extending international law to cryptocurrency. However, there are cogent barriers to its application and the first one is the prohibition of cryptocurrency in some countries. It is reported that more than 40 countries have banned or restricted the transaction and ownership of cryptocurrency (Economic Times, 2022). The adoption of GATS with this existing dynamism in the cryptocurrency market could imply that there is a barrier to free trade, and this could cause legal dissonance between treaty and the legislative decisions of the countries that banned cryptocurrency. Another barrier is that the continuous evolution of blockchain-enabled technologies may create platforms that negate viewing blockchain wholly as a service and not a product. An instance of this non-fungible tokens (NFTs) which are reliant on cryptocurrency infrastructures. It would be fundamentally incorrect to refer to NFTs as services because they are artworks (drawings, paints, graphic arts, videos, pictures, etc) which are commonly construed as goods; and NFT marketplaces accept cryptocurrencies to facilitate transactions such as NFT purchases and borrowing (Temi, 2022). This problem of taxonomy in cryptocurrency and digital assets is discussed extensively in Allen et al., (2020). Lastly, it is important to note that GATS only applies to World Trade Organisation members: at the present time, there are 14 non-WTO countries including Monaco, Eritrea, the Palestinian and Kosovo; and there are 25 countries that are still in the process of becoming WTO countries such as Iran, Ethiopia, Belarus and Bosnia (Amadeo, Kelly, & Binder, 2021).

Beyond the construct of the technological infrastructure that sustains cryptocurrency, judging cryptocurrency's legal nature as an entity is another discourse that appears in literature. According to Cherniei et al., (2021) in their discussions on the criminal liability for cryptocurrency transactions, the extension of any body of law to cryptocurrency (especially in the case of global transactions) would require all types of cryptocurrencies to be legally identified as a property – better still, as a form of money. It is in this light that some associations or legal opinions refer to cryptocurrency as "digital money" (Perkins, 2020, p. 1). This implies that the law of a nation – and if accepted among international bodies, the international law – considers all forms of cryptocurrency such as Bitcoin, Ethereum and Dogecoin as legal tenders for commercial activities. In an extreme opinion, this would also imply that the rejection of cryptocurrency in return for goods or services may be considered illegal.

However, the legal identification of cryptocurrency as a form of money that people use for private transactions has not equalled it for a legal tender – such as Naira, Dollar, and Pound Sterling – in some countries. An instance of this is found in Spain where the government recognises cryptocurrency only as "private" system of payment which implies that they are legally supported as a tender for exchange between private

parties but not a public legal tender (Cherniei, Cherniavskyi, Babanina, & Tykhonova, 2021). Another instance is found in Argentina where the government also makes the transaction of cryptocurrency legal, but it is not identified as a legal currency and tender – that is, it can be rejected in commercial exchanges (Ehret & Hammond, 2021). In addition, except there will be conditional clauses that can be understood by every layman, it is not exactly advisable to make cryptocurrency a legal tender in a country. The reasons are numerous but mainly: all types of cryptocurrencies are generally unstable and are beyond the management of national authorities; and, secondly, many cryptocurrency projects have been proven to be scams over the years and this could negatively affect national security if they were identified as legal tenders (European Security and Market Authority, 2022).

It is important to note that there have been increases in the development of "stablecoins" which refer to types of cryptocurrencies that have stable and uniform market values like traditional currencies (Arner, Auer, & Frost, 2020). Stablecoins are developed by connecting their value to traditional currencies with sustainable values such as the United State Dollars or commodities such as gold (CFI Teams, 2022). A major example of stablecoins is Tether which is also called USDT and its value is linked with the United States Dollar (CFI Teams, 2022). However, these forms of cryptocurrency do not enjoy popular adoption and use like Bitcoin and Ethereum because they do not offer significant profits or returns on investment as their value is static (Davis, 2022). This sole market dynamism constitutes a barrier to the extension of international law, as larger volumes of transactions are done with cryptocurrencies whose values are not regulated.

In Emelianova and Dementyev (2020), the development of a modern approach to tackle the extension of international law to cryptocurrency regulation which focuses on fostering cooperation among states is examined. The authors, however, posit that there are diverse challenges and barriers in the extension of international to cryptocurrency. A cogent factor that is emphasised is that the lack of a uniform approach to the regulation of the cryptocurrency market among states forms a significant barrier to the extension of international law to its regulation. Thus, the implication of Emelianova and Dementyev's (2020) stance in line with the foregoing discussions in this paper is that there is the need to develop new international law frameworks as regards the regulation of cryptocurrency markets. In theory, this will enable states and international bodies to address specific barriers to the regulation of cryptocurrency markets and matters that ensue from the transaction of cryptocurrency at the international level, and it will also enable nations to reach common grounds on the regulation of cryptocurrency markets.

Morton (2020) examines views that are similar to the provisions of Emelianova and Dementyev (2020). According to the author, the inconsistencies in the considerations of the application of international to cryptocurrency and the disparities in the national regulatory frameworks for cryptocurrency form barriers to the successful extension of international law to the regulation of cryptocurrency markets. To this end, Morton (2020) avers that nations need to come together to develop a unified framework for the regulation of virtual currencies. The study lays specific emphasis on curbing the level of cross-

border criminal activities, such as fraud, that are executed via cryptocurrency systems. Morton (2020) further promotes the position that a central international regulatory framework for cryptocurrency marketplaces can achieve the successful application of international law to cryptocurrency.

The following discussions on the digital nature of cryptocurrency (which challenges the enforceability of international law), and the need to develop an international regulatory framework that has the support of all states and stakeholders is reflected in the study by Aleksandrina (2021). The author identifies the infrastructure of smart contracts in cryptocurrency markets which facilitates successful peer-to-peer transactions, and, as such, remains an important aspect in cryptocurrency which needs to be considered in regulatory frameworks. Aleksandrina (2021) expresses two major challenges in the application of the principles of international private law to smart contracts (and cryptocurrencies): (1) the traditional criteria for determining a civil contract or a foreign economic transaction are not inherently applicable for smart contracts; and (2) there is no uniform legal understanding of smart contract across different national regulatory frameworks. Thus, the first step in successfully extending international law to cryptocurrency is to initiate a transformation of the law's principles and framework to reflect dynamics of blockchain technology, cryptocurrency and important features of cryptocurrency markets such as peer-to-peer transactions and smart contracts (Aleksandrina, 2021). In addition to this, a uniform approach to the regulation of cryptocurrency markets among nations needs to be promoted to achieve the enforceability of international law across regions.

In this subsection, this paper examined the extension of international law to cryptocurrency as a step towards achieving the global regulation of cryptocurrency and enabling international law to address issues such as conflict resolution or taxation that are related to cross-border cryptocurrency transactions. It is seen that it is highly challenging to apply international law to cryptocurrency at the current time because of several issues. Some include disparities in national regulatory frameworks on cryptocurrencies, smart contracts do not fit into the traditional criteria for determining a foreign economic transaction and a civil contract, and treaties such as GATs do not reflect on the innovative nature of cryptocurrency markets and the blockchain technology. Further discussions express that the development of an international law framework that enjoys popular acceptance among nations – which means there will be uniformity among national cryptocurrency regulatory frameworks and the international framework – and stakeholders, such as cryptocurrency companies, can be used to achieve an international regulatory framework where international law will be enforceable in cryptocurrency markets.

According to Salami (2018), the international law for regulating cryptocurrency markets needs to reflect on diverse technical, legal and security requirements. Some these include customer due diligence (CDD)/ know your customer (KYC) practices, anti-money laundering (AML) systems, and countering the financing of terrorism (CFT) systems. The law, in conjunction with cryptocurrency companies, relevant technology, financial and security organisations and all willing countries,

needs to develop a central standard for all those requirements and their regulations. This will have significant benefits across the world. One of them is the feasibility of utilising international law to combat international money laundering practices that are committed via cryptocurrency systems (Holman & Stettner, 2018; Velkes, 2020; Campbell-Verduyn, 2018). This will also enable nations to address the use of cryptocurrency to avoid taxation in organisational/individual cross-border transactions (Emelianova & Dementyev, 2020). In the same vein, Macfarlane (2020) argues that the development of an enforceable international law for cryptocurrency can enable international organisations to curtail the use of cryptocurrency to evade international economic sanctions. Lastly, it will also improve how nations address and overcome the use of cryptocurrency to fund and facilitate terrorist activities which has grown to be a highly concerning practice in the recent times (Keatinge, Carlisle, & Keen, 2018; Dion-Schwarz, Manheim, & Johnston, 2020).

2.1 Theoretical Model

There have been varied discussions on the development of legal regulations for technology, yet there are limited theoretical considerations on the link between law and technology or the effects that technological advancements have on law. However, researchers such as Moses (2007), Cockfield and Pridmore (2007), Cockfield (2004), Friedman (2001) and Easterbook (1996) discuss extensively on moving towards a theory for considering the link between technology and law.

A starting point for theorising a relationship between technology and law is understanding the effects of technology on law (Friedman, 2001). Friedman (2001) further outline three ways by which technology influence law, these include:

1. by altering the cost of violating and enforcing existing legal rules;
2. by altering the underlying facts that justify legal rules; and
3. by changing the underlying facts implicitly assumed by the law, making existing legal concepts and categories obsolete, even meaningless.

These points from Friedman (2001) focus primarily on how technology may lead to exploring the vulnerabilities in existing legal provisions and how technology may affect the applicability of law. This is because technology, depending on what time, can revolutionise several social interactions and the modes of operations in different spheres. This issue is highlighted in Moore (2019) where it is stated that new technology poses a challenge for traditional legal processes as the framework guiding those processes may not be intrinsically applicable to the new technology. From this viewpoint, it can be understood that theoretical perspectives on the relationship between law and technology need to include a reflection on how technology can inform legal processes and their application.

Another author considers how technology can affect law in a slightly related manner with Friedman (2001). Moses (2007) identifies four ways in which technology can pose new difficulties for law, they include:

1. the potential need for laws to ban, restrict or, alternatively, encourage a new technology;
2. uncertainty in the application of existing legal rules to new practices;
3. the possible over-inclusiveness or under-inclusiveness of existing legal rules as applied to new practices; and

4. alleged obsolescence of existing legal rules.

These points from Moses (2007) capture the legal considerations of cryptocurrency in different jurisdictions: banned or prohibited in some countries, restricted in some countries, and encouraged in other countries. The theoretical perspective presented by Moses (2007) also questions the extent to which the existing legal frameworks can effectively encompass all aspect of the new practices that arise from a new technology. For example, it is questionable if existing laws can effectively address all actions and transactions that are enabled on the blockchain technology such financial transactions, the public accessibility of transaction blocks or details, non-fungible digital arts and blockchain-enabled security framework.

The issue on the applicability of law for different aspects of technology has created two broad arguments on the development of theoretical models for technology and law. The first argument is the development of different or multiple theories for understanding the relationship of different technologies with the law (Easterbook, 1996). Easterbook (1996) is of the opinion that there are no general non unified practices in the impacts of different technology advancements on law. For this purpose, different theories should explain the relationship between each type of technology and the law. However, this is a time and resource exhausting perspective given the rapid growth of technology as well as the different legal response to technology across countries.

The second argument by Cockfield and Pridmore (2007) and Cockfield (2004) opines for the development of a general argument for explaining the relationship between technology and law. This approach considers it critical to jointly consider how technology inform legal practices and legal frameworks, regardless of the type of technology (Cockfield, 2004). Given the multiplicity in the use of cryptocurrency, this argumentative perspective on a theory for technology and law appears more practical.

In the model for a general theory of technology and law that was developed by Cockfield (2004), there are three components which include (1) law and technology relationship, (2) use behaviour, whether by at the group or at the individual level; and (3) policy outcomes.

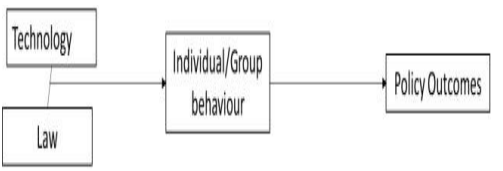

Figure 1: A general theory of technology and law (Cockfield, 2004).

The first component is relevant for understanding if the technology in question can be regulated using the existing legal framework or its beyond the scope of the framework. This will determine the relationship between the technology and law, and the form of legal response to the technology (Cockfield and Pridemore, 2007). The relationship between technology and law further affects human behaviour in the use of the technology such that legal prohibition may lead to illegal and unethical usage while regulated usage may promote a legal use behaviour. Lastly, Cockfield (2004) opines that the observed behaviour of use technology should influence well-thought policies. A critical implication of this assertion is that policies that regulate the use of technology should be informed by the observed practices – both legal and illegal – among users in order to develop

regulations that truly reflect the impacts of the technology.

This general theory of technology and law is applicable in the context of the relationship between international law and cryptocurrency, and its impacts on Nigeria. This is because there is currently no policy regulating cryptocurrency at the international level but there are observed use behaviours of cryptocurrency at international level and in Nigeria. Thus, our observation of the gap in policy can be addressed by considering the individual and group behaviour in the use of cryptocurrency. The application of this general theory of technology and law in the present paper is in figure 2 below.

Figure 2: Theoretical model, adapted from Cockfield (2004).

3. Effect of Extending International Law to Cryptocurrency on Nigeria's National Security

Nigeria provides a distinctive case of cryptocurrency market. The Nigerian government prohibits the use of cryptocurrency, and this prohibition is enforced by using banks to monitor and flag cryptocurrency related deposits and payments (Smith, 2022; Nwanisobi, 2021). Despite this legal prohibition of cryptocurrency, reports show that there have been increasing cryptocurrency transactions, ownership, and use of cryptocurrency-related technologies such as NFTs in Nigeria (Smith, 2022). Premium Times (2021) attributes the continued boom of the cryptocurrency market, despite the ban, to the existing volume of cryptocurrency ownership, citizens use of cryptocurrency to avoid the effects of the Naira devaluation over the time, cryptocurrency selling and management as a form of self-employment, and the use of cryptocurrency to achieve seamless cross-border transactions. Surprisingly, the Nigerian government launched a digital currency called "eNaira" after banning cryptocurrency as a form of home-grown and regulated digital money, but the Central Bank of Nigeria noted that the eNaira does not use the blockchain/cryptocurrency infrastructure (Chukwuere, 2021).

The Nigeria government banned cryptocurrency on the grounds that it enables criminals to transact outside the systems that are within the purview of governmental control, and, as such, criminals go unnoticed (Premium Times, 2022). The criminal activities with national threat possibilities that raised major concerns for the Nigerian government include terrorism and kidnapping (Sahara Reporters, 2021; Maza, Koldas, & Aksit, 2020). However, it appears that the ban on cryptocurrency only worsened the extent to which these criminal activities are perpetrated through cryptocurrency outside the reach of Nigerian financial regulatory and security bodies. Prior to banning cryptocurrency markets in Nigeria, liquidating cryptocurrency into Naira or other currencies in Nigeria was simply done through exchanging cryptocurrencies on market platforms to the traditional currencies and transferring them to Nigerian bank accounts. However, the ban on cryptocurrency made users, including those used for criminal and non-criminal purposes, to resort into the use of black-market systems, which facilitates the liquidation of cryptocurrencies outside the Nigerian financial system regulatory routes (Premium Times, 2022).

What can be deduced from the empirical case above is that banning cryptocurrency

has not helped Nigeria in fighting the illegal activities that are committed through cryptocurrency – in fact, it worsened the activities and kept them out of the detection of relevant authorities. Asides the ostensive national security effects of cryptocurrency in Nigeria, it also could influence economic-related security issues in Nigeria as Ahannaya et al., (2021) assert that the adoption of cryptocurrency in Nigeria continuously increases and this may challenge the status of the Naira, especially in view of its continued devaluation. These show that the cryptocurrency market has a significant stand among Nigerians and in the Nigerian economy. From another point of view, Fakunmoju et al., (2022) argue that cryptocurrency channels are used to perpetrate corrupt practices such as public fund siphoning and money laundering which have negative effects on the country's economy.

While Nigeria is not the only country to have banned cryptocurrency, the outlined and discussed dynamics of the cryptocurrency market in Nigeria show that the legal prohibition of cryptocurrency is not the most effective approach to cryptocurrency regulation in the country. Alternatively, the country should develop a robust regulatory framework that legalises and monitors its use (Ahannaya, Oshiowo, Sanni, Arogundade, & Ogunwole, 2021). Within the context of this study, the development of a national regulatory framework for cryptocurrency in Nigeria that supports the extension of international law to the regulation of cryptocurrency is key. The succeeding discussions examine the effects that this may have on the national security in Nigeria.

3.1. Curtailing Terrorism Funding

As identified earlier, terrorism is one of the major criminal activities that is funded through cryptocurrency channels in Nigeria. This security challenge is also a global issue. According to Wardhana and Nugroho (2021), cryptocurrency is an alternative financial system that facilitates user-controlled assets and user-to-user transactions without middlemen and regulatory oversight functions. This has enabled terrorist organisations across the world to conduct transactions and payments that support their illegal acts without being caught by security authorities (Wardhana & Nugroho, 2021). Essentially, cryptocurrency forms a financial system that terrorists use to evade detection and fundraise their crimes. The current use of black markets to liquidate cryptocurrencies in Nigeria due to legal prohibition further strengthens the evasion of being detected by relevant Nigerian anti-terrorist and security organisations.

The depth of the evasion of authorities in Nigeria by terrorists – and other criminals such as kidnappers – through the use of cryptocurrencies after the ban is expressed in the report by Premium Times (2022). It is noted that these criminal organisations are now able to transact freely, outside of the radar of Nigerian authorities through cryptocurrency and black-market liquidation. Not only has this reduced the extent to which relevant authorities can detect suspicious financial transactions, it has – by implication – increased the rates of the perpetrations of these illegal and harmful activities (Premium Times, 2022). The continuance of this could have severe effects on the national security of Nigeria. The ease of funding and criminal transactions accelerates the growth and infiltration of criminal organisations such as kidnappers and terrorists.

The development and implementation of an international law framework that regulates cryptocurrency, given that Nigeria subscribes to it instead of

prohibiting cryptocurrency, can assist the country in the fight against terrorism and kidnapping – especially terrorism, as it is a more significant national security threat. According to Salami (2018), the extension of international law to cryptocurrency has the capacity to curtail the actions of terrorist organisations in Nigeria as well as other parts of the world. The international regulatory framework will not only enhance the detection and investigation of suspicious and terrorist-linked cryptocurrency transactions, but it will also facilitate the enforcement of the law to convict cross-border participants in the transaction. Through this, Nigeria will be able to clamp down on the rising level of terrorist threats in the country.

In the same vein, a report from the office of the Attorney General, Washington D. C, (2022) expresses that strengthening international law in the regulation of digital assets such as cryptocurrencies is important for combating terrorism and other criminal activities that could be planned or funded through cross-border interactions. The report discusses that the nature of digital assets mitigates the level to which criminal transactions that are initiated through them can be investigated and further notes that cooperation between international law and relevant technology companies in the digital asset industry can strengthen legal attempts to combat and investigate criminal digital asset transactions. A key contribution of this report is that using international law to regulate cryptocurrency enables countries to seek the cooperation of cryptocurrencies companies that are not within their jurisdiction to conform to the requirement of law in an investigation. The implication of this for Nigeria is that the country can deploy international law to seek the complete cooperation of a cryptocurrency company for the provision of all relevant details in the investigation of a suspicious or a terrorism-related cryptocurrency transaction. This will positively affect tackling terrorism funding through cryptocurrency in the country.

Lastly, in Iyoyojie et al., (2021), the relevance of a global regulatory framework in addressing the security issues that are associated with cryptocurrencies across the world is emphasised. The authors discuss that the extension of international law to the regulation of cryptocurrency can provide universal reference law for user registration, company licencing and responsibilities of companies in cases of criminal investigations. Such law will offer Nigeria a legal platform for detecting and investigating transactions that are done in support of terrorism and other criminal activities such as kidnapping; and the law will also provide prosecution frameworks for both indigenous and foreign transgressors.

3.2. Maintaining Economic Performance

According to Fakunmoju et al., (2022), in their empirical examination into the effects of cryptocurrency trading and monetary corrupt practices on Nigerian economic performance, cryptocurrency trading facilitates large volumes of monetary corrupt practices, and this has significant negative effects on the country's economic performance. To curb this outcome, the authors suggest that the Nigerian government needs a comprehensive regulatory approach to the cryptocurrency market in Nigeria that monitors and controls cryptocurrency trading – not a regulatory framework that prohibits cryptocurrency. The implication of these authors assertions, especially in the light of the use of black-markets to liquidate cryptocurrency assets due its prohibition, is that the

unregulated nature of the cryptocurrency market in Nigeria enables individuals and organisations to achieve financial corruption and frauds through cryptocurrency trading which further negatively affects the economy of the country.

Wawrosz and Lansky (2021) also reveal that cryptocurrencies have been adopted as a means of enacting successful financial crimes and evade the law. The authors note that the nature of cryptocurrency, especially without regulations, enables individuals and organisations to transact large sums of money that were siphoned in an undetectable way to relevant government authorities. Kataryzna (2019) also posits that the use of cryptocurrency for corruption has grown to become a global issue. Among the diverse corrupt practices in which cryptocurrency could be utilised which could affect the economy of Nigeria, tax evasion and money laundering are leading cases (Katarzyna, 2019; Onyeke, 2020).

According to Okpalaojiego (2021), the Nigerian government's prohibition of cryptocurrency as a response to the corrupt and criminal activities that are done via it has only worsened the use of cryptocurrency for illicit financial activities and, by implication, the impact the corrupt and criminal activities on the country's economy also heightens. The positions of the authors also show that the ban of cryptocurrency in Nigeria has made it impossible for the country to tax profits and transactions made through cryptocurrency markets in Nigeria. This implies that the country needs to employ pragmatic regulatory frameworks for the usage of cryptocurrency which identifies it as a form of personal commercial tender, controls its use and taxes profits that are made through its trading.

The extension of international law to the regulation of cryptocurrency can help Nigeria to effectively monitor and regulate the cryptocurrency market in its region with focus on reducing the rate of money laundering and tax evasion crimes that are committed through the market. Additionally, the development of an enforceable international law on cryptocurrency regulation will enable Nigeria to legally act on cross-border financial corruption crimes that affect the nation's government, organisations, or individuals.

4. Conclusion

The lack of a central legal framework for the regulation of cryptocurrency at the international level has allowed the perpetration of illicit activities through cryptocurrency channels without being detected or successfully prosecuted. Countries across the world have adopted different extremes to the regulation of the cryptocurrency market. An extreme is the promotion of the adoption of and spending of cryptocurrency; and the other extreme is the prohibition of cryptocurrency. Regardless of the regulatory stances of countries on the cryptocurrency market, what remains peculiar is that the adoption of cryptocurrency keeps growing and so does its use for illegal activities getting sophisticated at both national and cross-national levels. As such, the need for a uniform legal framework for the regulation of cryptocurrency at the international level is emphasised in this study. This will enable nations and international bodies to clamp down the illegal activities that are conducted via cryptocurrency and address contractual and conflict resolution issues that arise from international cryptocurrency transaction.

Nigeria presents a case where cryptocurrency was banned and yet, its adoption has been increasing and its

prohibition has worsened its use for illegal activities that threaten national security and economic health. Individuals and organisations have found ways to trade and own cryptocurrencies in the country without getting detected by relevant authorities in the country. By implication, Nigeria needs to re-consider its stance on cryptocurrency regulation. Most importantly, the development of an international regulatory framework that facilitates the successful extension of international law to the regulation of cryptocurrency can help Nigeria to improve its national security by tackling terrorist and other crime funding and tackling the use of cryptocurrency for corrupt practices such as money laundering and tax evasion.

This paper calls on relevant international bodies and state governments to collaborate with cryptocurrency firms and strategize towards the development of an international regulatory framework for cryptocurrency.

5. Recommendations

For Nigeria and a host of other countries, a reliable and enforceable international law to probe cryptocurrency-related cases is key to addressing many national security threats and promoting the interest of their citizens, public and private organisations as related to the cryptocurrency markets. Also, the enforceability of international law in the regulation of cryptocurrency will provide international organisations the capacity to address international level crimes and cases where international economic sanctions are evaded through cryptocurrency. To achieve such enforceable international law in the cryptocurrency landscape, this paper recommends that stakeholders need to agree to the development of a new international regulatory framework that reflects on the dynamics of cryptocurrency and blockchain – as existing traditional international law may not inherently be applicable to cryptocurrency dynamics such as smart contracts and decentralisation.

The stakeholders that will be involved in this agreement include international security, legal and economic organisations such as World Trade Organisation, United Nations (UN), Organization for Economic Co-operation and Development (OECD) and the International Law Commission; countries; and global cryptocurrency organizations. These stakeholders should deliberate on an international law framework that encompass the security, corrupt practices and regulatory issues in cryptocurrency markets which will form a reference regulatory system for each country. The international regulatory framework should emphasise the development and implementation of comprehensive CDD/KYC, AML, and anti-crime funding systems. These will ease crime detection and investigative processes.

With specific focus on Nigeria, the government needs to revisit its existing prohibition of the cryptocurrency. It has been shown that the ban has led to the adoption of evasive channels for liquidating cryptocurrency which promotes higher rates of criminal activities through cryptocurrency. Thus, reconsiderations on legalising and regulating the usage of cryptocurrency should be promoted in the country. A comprehensive legislative framework that monitors and controls cryptocurrency trading and ownership in Nigeria will yield more positive economic and security outcomes such that using cryptocurrency to fund terrorism and kidnapping or using it to launder public funds can be reduced. To achieve such regulatory framework, the

Nigerian government needs to partner with leading cryptocurrency marketplaces and key opinion leaders in the nation. This will facilitate the development of applicable regulations and promotion among the populace to achieve popular acceptance. It is also important to note that in the case of the development of an international law that regulates cryptocurrency in the future, Nigerian prohibition of cryptocurrency may make it difficult to apply the law to the benefit of the nation. Hence, its acceptance and regulation hold higher prospects for the nation.

References

Ahannaya, C. G., Oshiowo, A. D., Sanni, A. S., Arogundade, J. A., & Ogunwole, O. J. (2021). The effect of cryptocurrencies on nigeria economy. *IEEE-SEM*, *9*(3), 8-14.

Akkus, H. T., Gursoy, S., Dogan, M., & Demir, A. B. (2022). Metaverse and metaverse cryptocurrencies (meta coins): bubbles or future? *Journal of Economics, Finance and Accounting, 9*(1), 22-29.

Al-Amiri, R., Zakaria, N. H., Habbal, A., & Hassan, S. (2019). Cryptocurrency adoption: current stage, opportunities, and open challenges. *International Journal of Advanced Computer Research, 9*(44), 293-307.

Aleksandrina, M. (2021). Transformation of the principles of international private law in the digital age. *SHS Web Conference, 109*(01003), 1-6.

Allen, J. G.; Rauchs, M.; Blandin, A.; Bear, K. (2020, 2020). *Legal and regulatory considerations for digital assets.* Retrieved November 3, 2022, from https://www.jbs.cam.ac.uk/wp-content/uploads/2020/10/2020-ccaf-legal-regulatory-considerations-report.pdf

Amadeo, K., Kelly, R. C., & Binder, J. (2021). *How does a country become a WTO member?* Retrieved November 3, 2022, from https://www.thebalancemoney.com/how-does-a-country-become-a-wto-member-3306362

Ante, L. (2022). Non-fungible token (NFT) markets on the Ethereum blockchain: temporal development, cointegration and interrelations. *Economics of Innovation and New Technology*, 1-10.

Anthony, B. (2021, March 06). *Distributed ledger and decentralised technology adoption for smart digital transition in collaborative enterprise.* Retrieved October 08, 2022, from https://www.tandfonline.com/doi/full/10.1080/17517575.2021.1989494

Arner, D., Auer, R., & Frost, J. (2020). *Stablecoins: risks, potential and regulation.* Basel: Bank for International Settlements.

Campbell-Verduyn, M. (2018). Bitcoin, crypto-coins, and global anti-money laundering governance. *Crime Law Soc Change, 69*, 283–305.

CFI Teams. (2022). *Stablecoin*. Retrieved November 3, 2022, from https://corporatefinanceinstitute.com/resources/cryptocurrency/stablecoin/

Cherniei, V., Cherniavskyi, S., Babanina, V., & Tykhonova, O. (2021). Criminal liability for cryptocurrency transactions: global experience. *European Journal of Sustainable Development, 10*(4), 304-316.

Chukwuere, J. E. (2021). The eNaira - opportunities and challenges. *Journal of Emerging Technologies, 1*(1), 72-77.

Davis, C. (2022). *Top stablecoins & types of stablecoins*. Retrieved November 3, 2022, from https://www.benzinga.com/money/best-stablecoins-and-4-types-of-stablecoins

de Best, R. (2022). *Daily 24h volume of all crypto combined up until August 18, 2022* . Retrieved October 7, 2022, from https://www.statista.com/statistics/12729

03/cryptocurrency-trade-volume/

Dion-Schwarz, C., Manheim, D., & Johnston, P. B. (2020). *Terrorist use of cryptocurrencies.* Santa Monica, Calif: RAND Corporations.

Economic Times. (2022). *Economic Times*. Retrieved November 3, 2022, from https://economictimes.indiatimes.com/news/web-stories/countries-which-have-banned-or-restricted-use-of-cryptocurrency/slideshow/89153960.cms?from=mdr

Ehret, T., & Hammond, S. (2021, June 1). *Compendium – Cryptocurrency regulations by country.* Retrieved November 3, 2022, from https://www.thomsonreuters.com/en-us/posts/wp-content/uploads/sites/20/2021/06/Compendium_Cryptocurrency-Regs_FINAL.pdf

El Faqir, Y., Arroyo, J., & Hassan, S. (2020). An overview ofdecentralized autonomous organizations on the blockchain. New York: OpenSym 2020: 16th International Symposium on Open Collaboration.

Emelianova, N. N., & Dementyev, A. A. (2020). Cryptocurrency, taxation and international law: contemporary aspects. In E. G. Popkova, & B. S. Sergi (Eds.), *Advances in inteligent system and computing* (pp. 725-731). Switzerland: Springer.

European Security and Market Authority. (2022). *Crypto-assets and their risks for financial stability.* Paris: European Securities and Markets Authorit.

Fakunmoju, S. K., Banmore, O., Gbadamosi, A., & Okunbanjo, O. I. (2022). Effect of cryptocurrency trading and monetary corrupt practices on nigerian economic performance. *Binus Business Review, 13*(1), 41-40.

Guillame, F. (2019). Aspects of private international law related to blockchain transactions. In E. Kraus, T. Obrist, & O. Hari (Eds.), *Blockchains, smart contracts, decentralised autonomous organisations and the law* (pp. 49-82). UK, USA: Edward Elgar Publishing Limited.

Guillaume, F., & Riva, S. (2022, March 28). *Blockchain dispute resolution for decentralized autonomous organizations: the rise of decentralized autonomous justice.* Retrieved September 2, 2022, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4042704

Holman, D., & Stettner, B. (2018). *Anti-Money laundering regulation of cryptocurrency: U.S. and global approaches.* Retrieved November 3, 2022, from https://www.allenovery.com/germany/-/media/sharepoint/publications/publications/en-gb/documents/aml18_allenovery.pdf

Iyoyojie, L. D., Edeh, O. J., Erinne, U., & Umezurike, C. (2021). Cryptocurrency: the search for a legal framework as a world currency. *International Journal of Business & Law Research, 9*(3), 15-25.

Katarzyna, C. (2019, March 20-21). Cryptocurrencies: opportunities, risks and challenges for anti-corruption compliance systems. *2019 OECD Anti-corruption & Integrity Forum*, pp. 1-15.

Keatinge, T., Carlisle, D., & Keen, F. (2018). Virtual currencies and terrorist financing: assessing the risks and evaluating responses. Brussels: European Union.

Liu, Y., & Tsyvinski, A. (2021). Risks and returns of cryptocurrency. *The Review of Financial Studies, 34*(6), 2689-2727.

Macfarlane, E. K. (2021). Strengthening sanctions: solutions to curtail the evasion of international economic sanctions through the use of cryptocurrency. *Michigan Journal of International Law,*

42(1), 199-232.
Maza, K. D., Koldas, U., & Aksit, S. (2020). Challenges of combating terrorist financing in the Lake Chad region: A case of Boko Haram. *SAGE Open, 1*, 1-17.
Miraz, M. H., & Ali, M. (2018). Applications of blockchain technology beyond cryptocurrency. *Annals of Emerging Technologies in Computing, 2*(1), 1-6.
Morton, D. T. (2020). The future of cr e of cryptocurrency: an unr ency: an unregulated instrument in an increasingly regulated global economy. *Loy. U. Chi. Int'l L. Rev, 16*(1), 1-16.
Mukhopadhyay, U., Skjellum, A., Hambolu, O., Oakley, J., Yu, L., & Brooks, R. (2016). A brief survey of cryptocurrency systems. Auckland: IEEE.
Munoz, J. G. (2020). 'Crypto-Investment' in international economic law: a first sketch. *Global Jurist, 20*(2), 1-13.
Narain, A., & Moretti, M. (2022). *Regulating crypto*. Retrieved September 9, 2022, from https://www.imf.org/en/Publications/fandd/issues/2022/09/Regulating-crypto-Narain-Moretti
NotaBene. (2022). *Crypto travel rule in Japan by the Financial Services Agency (FSA)*. Retrieved 3 October, 2022, from https://notabene.id/world/japan
Nwanisobi, O. (2021). *Response to regulatory directive on cryptocurrencies*. Nigeria: Central Bank of Nigeria.
Office of the Attorney General, Washington D. C. (2022). How to strengthen international law enforcement cooperation for detecting, investigating, and prosecuting criminal activity related to digital assets. Washington D. C.: U.S Department of Justice.
Okpalaojiego, E. C. (2021). Effects and implications of crypto currency ban on Nigerian economy. *Academic Journal of Current Research, 8*(4), 23-34.
Onyeke, C. E. (2020). Crypto-currency and the nigerian economy: problems and prospects . *IAA Journal Of Social Sciences, 6*(1), 152-162.
Ozili, P. K. (2022). Central bank digital currency in Nigeria: opportunities and risks. In S. Grima, E. Ozen, & H. Boz (Eds.), The New Digital Era: Digitalisation, Emerging Risks and Opportunities (Contemporary Studies in Economic and Financial Analysis, Vol. 109A) (pp. 125-133). Bingley: Emerald Publishing Limited.
Perkins, D. W. (2020). *Cryptocurrency: the economics of money and selected policy issues*. Washington D.C.: Congressional Research Service.
Politou, E., Casino, F., Alepis, E., & Patsakis, C. (2021). Blockchain mutability: challenges and proposed solutions. *IEEE Transactions on Emerging Topics in Computing, 9*(4), 1972-1986.
Premium Times. (2021). *Why crypto is booming in Nigeria despite govt ban*. Retrieved Novovember 5, 2022, from https://www.premiumtimesng.com/promoted/483386-why-crypto-is-booming-in-nigeria-despite-govt-ban.html
Premium Times. (2022). *Nigeria's crypto banking ban: One year later, By Olaoluwa Samuel-Biyi*. Retrieved November 5, 2022, from https://www.premiumtimesng.com/opinion/510293-nigerias-crypto-banking-ban-one-year-later-by-olaoluwa-samuel-biyi.html
Sahara Reporters. (2021). *'It's fueling terrorism' – CBN speaks on why it banned cryptocurrency*. Retrieved November 5, 2022, from https://saharareporters.com/2021/02/08/its-fueling-terrorism-%E2%80%93-cbn-speaks-why-it-banned-cryptocurrency
Salami, I. (2018). Terrorism financing with virtual currencies: Can regulatory

technology solutions combat this? *Studies in Conflict and Terrorism, 41*(12), 968-989.

Sanz-Bas, D., del Rosal, C., Alonso, S. L., & Fernandez, M. A. (2021). Cryptocurrencies and fraudulent transactions: risks, practices, and legislation for their prevention in Europe and Spain . *Laws, 10*(3), 1-14.

Smith, M. (2022). *Cryptocurrency usage soars in Nigeria despite bank ban*. Retrieved November 3, 2022, from https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/cryptocurrency-usage-soars-in-nigeria-despite-bank-ban-70497781

Temi. (2022). *Bridging fintech and blockchain: benefits, problems and solutions*. Retrieved October 7, 2022, from https://blog.cryptostars.is/bridging-fintech-and-blockchain-benefits-problems-and-solutions-2a1850a21ff

Temi. (2022). *The problems with Web3.0 and NFTs — Part 2*. Retrieved November 3, 2022, from https://blog.cryptostars.is/the-problems-with-web3-0-and-nfts-part-2-8dd4ce97f065

Velkes, G. C. (2020). International Anti-Money Laundering Regulation of Virtual Currencies and Assets. *International Law and Politics, 52*(4), 875-907.

Wardhana, A. T., & Nugroho, B. W. (2021). *Abuse of cryptocurrency to funding international terrorism activities.* Retrieved November 3, 2022, from https://prosiding.umy.ac.id/grace/index.php/pgrace/article/download/190/188/682

World Economic Forum. (2021, September). Navigating cryptocurrency regulation: an industry perspective on the insights and tools needed to shape balanced crypto regulation. Retrieved September 9, 2022, from https://www3.weforum.org/docs/WEF_Navigating_Cryptocurrency_Regulation_2021.pdf