UNDERSTANDING THE INTERRELATIVITY OF BLOCKCHAIN AND DATA PROTECTION IN NIGERIA

TABLE OF CONTENTS

CONTRIBUTORS

- 1. Ubochi Prince Ituma - Ebonyi State University
- 2. Akinnola Shalom - Adekunle Ajasin University
- 3. Boluwatife Alaran - University of Lagos
- 4. Abubakar Sadiq Tahir - Bayero University Kano
- 5. Joel Odili - University of Lagos
- 6. Ogunlade Olumide - Adekunle Ajasin University
- 7. Adeyinka - University of Ibadan
- 8. Nweke Chinonso - Ahmadu Bello University
- 9. Ayomikun Ogunjimi - Olabisi Onabanjo University
- 10. Onyeulor Adamma Joy - University of Benin

INTRODUCTION

Definition

Blockchain is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system.

Blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. Each block in the chain contains a number of transactions, and every time a new transaction occurs on the blockchain, a record of that transaction is added to every participant's ledger. Blocks are added continuously but never removed, hence it is classified as append only data structure. This cryptographic function makes the log tamper-evident, which increases transparency and accountability. The decentralized database managed by multiple participants is known as Distributed Ledger Technology (DLT).

Data protection on the other is the process of protecting data, which involves the relationship between the collection and dissemination of data and technology, the public perception and expectation of privacy and the political and legal underpinnings surrounding that data. It aims to strike a balance between individual privacy rights while still allowing data to be used for business purposes.

Dissenting from the foregoing, there has been several question as to the connectivity or strive between blockchain and data protection, this work focuses on their relativeness and association one with another.

LEGAL REGIME OF BLOCKCHAIN INTERNATIONALLY

Blockchain technology being one of the areas that is fast emerging, can be classified as part of the grey areas of law, which courtiers of the world have endeavor to create a legal reframe work to regulate the activities and usage of Blockchain in their counties. Over the years, countries of the world have openly admitted to the need for proper blockchain regulations and laws, the countries that allow the use of blockchain and cryptocurrency trading are currently using either indirect or direct ways to regulate their usage.

The direct regulation is when the laws governing the blockchain usage are officially introduced and enacted by government. It is indirect when the companies who use blockchain, have to follow the general regulation enacted by their countrries on general data protection.

Few of the countries of the world shall be used as example;

The United States

The United States is rightfully considered the most advanced country in the world in terms of blockchain and crypto currency adoption, with many businesses accepting crypto currency for their day-to-day operations. The complexity of U.S. laws lies in several governmental levels — federal and local (state) ones. While digital currency is recognized and legalized on a federal level, the laws may differ from state to state.

There are several federal agencies that regulate blockchain-related businesses in the United States. While they sound different, the following three classifications are very similar to each other and they allow several agencies to collaborate on regulatory and enforcement matters:

The U.S. Internal Revenue Service defines crypto currency as assets for taxation purposes.

The Commodities Futures Trading Commission (CFTC) defines crypto currency as a commodity.

The Securities and Exchange Commission distinguishes digital currency as a security.

Federal Trade Commission (FTC) went further and created a Blockchain Working Group, which primary goal is to crack down illegal and fraudulent schemes arising in the marketplace from time to time. Additionally, the Group also focuses on three more goals: building FTC staff expertise in crypto currency and blockchain technology assisting internal and external communication on enforcement actions and providing a forum for discussing potential influences on FTC’s objectives and how to respond to them

Malta

Malta, also known as the Blockchain Island, believes the potential of blockchain is endless. As part of their initiative to embrace this technology, the country has recently introduced two blockchain-related acts, known as Malta Digital Innovation Authority Act (MDIA ACT) and Innovative Technology Arrangement and Services Act (ITAS Act). MDIA Act focuses on certifying blockchain and establishing standards for the industry, while the ITAS Act focuses on setting up digital ledgers and regulating the entry of new blockchains.

Gibraltar

Gibraltar also was one of the first countries to adopt blockchain regulation. In fact, their initiative to regulate digital ledgers started back in 2014. Gibraltar's regulation is applied to exchanges, wallet providers, and all other business models working on a distributed ledger technology (DLT).

The country's DLT firms are regulated by the Gibraltar Financial Services Commission (GFSC). The DLT regulations came into effect on January 1, 2018, and provide nine main principles which each company working in the blockchain industry has to follow.

Belarus

Belarus was the first country in the world to create an official regulatory framework for the blockchain industry. In 2017, the president signed a decree focused on the blockchain and crypto currency-related innovations centered within the Hi-Tech Park (HTP), known as Belarusian 'Silicon Valley.'

The bill is called "Digital Economy Development Ordinance" and has been in effect since March 2018. According to the bill, the HTP has been designated as a special sector in the country, with special tax and legal regime for blockchain and crypto businesses. Companies-residents of the HTP are not restricted in issuing, storing or trading digital tokens. Furthermore, blockchain-centered companies that are members of the HTP get a tax break for the next five years, until 2023.

The other blockchain law imposed by the government in 2018 focused on the prevention of terrorism financing, money laundering, and propagation of weapons of mass destruction by means of any blockchain-related activities.

LEGAL REGIME OF BLOCKCHAIN IN NIGERIA

Nigeria presently has no specific legislation on Blockchain, however, can be classified under countries that adopt the indirect tactics in regulating the usage of Blockchain.

The laws include:

- The Investments and Securities Act 2007;
- The Central Bank of Nigeria (CBN) know-your-customer (KYC) and anti-money laundering/counter-terrorist financing (AML/CFT) policies;
- The Nigeria Data Protection Regulation 2019;
- The National Health Act;
- The Cybercrimes (Prohibition, Prevention, etc) Act 2015;
- The National Identity Management Act 2017;
- The Companies Income Tax Act;
- The Capital Gains Tax Act;
- The Personal Income Tax Act;
- The Value Added Tax Act;
- The Companies and Allied Matters Act;

- The Finance Act 2019;
- The Statute of Frauds 1677;
- The Evidence Act 2011;
- The Money Laundering (Prohibition) Act, 2011 (as amended);
- The Terrorism Prevention Act, 2012 (as amended);
- The Terrorism Prevention (Freezing of International Terrorist Funds and other Related Matters) Regulations, 2013;
- The Economic and Financial Crime Commission (Establishment) Act 2004; and
- The Banks and Other Financial Institutions Act 1991.

The Securities and Exchange Commission (SEC) is the apex regulatory body for the Nigeria capital market; it is empowered to regulate investments and securities business in Nigeria. In line with these powers, the SEC released a statement made on 14th of September 2020 on Digital assets and their classification and treatment. The commission issued regulation guidelines for digital currency and crypto-based companies is set to create standards that encourage ethical practices.

The Central Bank of Nigeria (CBN) has also enacted several policies through her know-your-customer (KYC) and anti-money laundering/counter-terrorist financing (AML/CFT) policies and other CBN regulatory frameworks, they include:

- The Three-Tier KYC Reqsuirements 2013;
- The Anti-money Laundering/Combating the Financing of Terrorism (Administrative Sanctions) Regulations 2018;
- The AML/CFT Policy and Procedure Manual 2018;
- The Consumer Protection for Banks and Other Financial Institutions 2016;
- The Consumer Protection Regulations 2019;

- The Guidelines on Mobile Money Services in Nigeria;
- The Guidelines on International Mobile Money Remittance Services;
- The Guidelines on International Money Transfer Services; and
- The Central Bank of Nigeria Act 2007.

LEGAL REGIME ON DATA PROTECTION

One of the leading regulation on Data Protection in the world is the EU General Data Protection Regulation, 2016. The regulation is on data protection and privacy in the European Union and the European Economic Area. It address issues such as transfer of personal data outside the EU, gives individuals powers and right over their personal data and regulate the activities of bodies make use of peoples personal data.

However, in Nigeria the National Information Technology Development Agency (NITDA) has commendably come up with the Nigeria Data Protection Regulations (NDPR) 2019, which specifically bothers on matters of data protection. The NDPR is an adaptation of the EU's GDPR, it touches on principle of data processing, the requirement of Data Compliance Officers, requirement of Data subject's consent for collecting and processing data, transfer of data and rights of data subjects and also prescribes penalty for non-compliance with the regulation.

The Constitution of Nigeria also serves as the foundation for data protection in Nigeria. The Constitution was the only the legal backup for Nigerians before the enactment of NDPR in 2019. The Constitution guarantees and protects rights of Nigerians to privacy with respect to their homes, correspondence, telephone conversations and telegraphic communications.

- Other laws in Nigeria that protect data and privacy right include;
- The NCC Consumer Code of Practice Regulation 2007;
- The Freedom of Information Act 2011;
- The Cybercrimes (Prohibition, Prevention, etc.) Act 2015;
- The Child Right Act 2003, etc.

RELATIONSHIP BETWEEN BLOCKCHAIN AND DATA PROTECTION

To understand the relationship between blockchain and data protection, the two terms must be understood separately first.

Blockchain is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system. A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. Each block in the chain contains a number of transactions, and every time a new transaction occurs on the blockchain, a record of that transaction is added to every participant's ledger.

Data protection is the process of protecting data, which involves the relationship between the collection and dissemination of data and technology, the public perception and expectation of privacy and the political and legal underpinnings surrounding that data. It aims to strike a balance between individual privacy rights while still allowing data to be used for business purposes.

THE RELATIONSHIP

It can be seen 'in a way' that Blockchain and Data protection are two sides of the same coin; they both have the same objectives, although it is a long run objective as Blockchain is a catalyst for data protection. Despite its potential for application as a means of enabling data protection by design, it is also a potential threat to the individual rights on data protection and privacy.

In May 2014, the European Court of Justice ruled that citizens of the EU were entitled to a claim against internet search engine operators to remove any content retrievable from the index of search results, as far as such referred to information on the individual concerned was of no particular significance for the public interest.

Although blockchain offers the advantages of transparency and immutability, it is these very characteristics that can lead to conflicts with data protection law. This is because blockchain as a catalyst of data protection, posits that a major way by which data can be protected is by sharing same with all parties involved, that way fraud or misinformation cannot be perpetuated without notice to all users, this in itself is a form of breach of privacy as all information or data concerning a user is made know to all other users and vice-versa.

The developers of blockchain projects should therefore carefully analyze the kind of data intended to be stored in the blockchain, and weigh up the advantages and disadvantages of the type of blockchain to be used. Certainly, the principles of data minimization and mechanisms for ensuring the anonymization of personal data are essential elements to consider, as blockchain seeks to protect the users by way of anonymity.

It wouldn't be surprising if companies engaging in use of blockchain technology will have to deal with the relevant regulatory framework, including data protection law. At the early stage in the development of any blockchain-based application, it is a must to ensure that its specific technical design meets the requirements set out by the applicable laws.

The EU has laws that regulate data protection; the General Data Protection Regulation's (GDPR), unfortunately GDPR and blockchain are not compatible because from a data protection perspective, the rise of the blockchain may be no less transformative. Whereas the GDPR was fashioned for a world where data is centrally collected, stored, and processed, while blockchain decentralize each of these processes. With a paradigm shift of such radical contours, we must enquire about the applicability of a legal framework constructed for a sphere of centralization to one of decentralization.

The Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation - "GDPR"), which entered into force in May 2018, provides that in addition to an approximation to the term blockchain (cf. section I.), the main question addressed by this article is, to what extent will this technology impact on those areas of life that have been traditionally regulated by analogue law and institutions (cf. section II.). Finally, the potential of blockchain is briefly addressed as an instrument of data protection (cf. section III.) and explains the extent to which data protection law may create certain boundaries to potential applications of blockchain technology (cf. section IV.)

CONCLUSION

From the forgoing, it can be deduced that blockchain has one of its major aims to be; data protection. However proper care and steps need to be put in place to ensure that there is no conflict of interest in its operation. Thus the need for a clear cut regulation, which will harmonize blockchain and data protection, without infringement on the right of its users ; blockhain should be determined within the scope of Data Protection.

REFERENCES

- Antonopoulos A (2017), Mastering Bitcoin O'Reilly, xxiii
- https://www.techopedia.com/definition/29406/data-protection
- OpenLedger Insights: Blockchain And The Law: Regulations Around the WorldPosted by Darya Yafimava | Jan 17, 2019 | Blockchain insights
- Section 13 of the investment and securities Act, 2007
- General Data Protection Regulation, Wikipedia.
- Review of the NDPR, "The New Law" by YimikaKetiku and DolapoBolu, available online at: http://www.spaajibade.com/resources/data-protection-regulation-2019-the-new-law-yimika-ketiku-and-dolapo-bolu accessed December 8, 2020.

REFERENCES

- Section 37, 1999 constitution of the federal republic of Nigeria.
- Case of Bar. EzugwuEmmaanuelAnene v. Airtel Nigeria Ltd. FCT/HC/CV/%$%/2015 (unreported)
- https://www.euromoney.com/learning/blockchain-explained/what-is-blockchain
- https://www.techopedia.com/definition/29406/data-protection
- https://www2.deloitte.com/dl/en/pages/legal/articles/blockchain-datenschutzrecht.html
- https://poseidon01.ssrn.com/delivery.php?ID=774106069097103097017031024081015065099038066037028071088064110088127003089021 1
- Case of Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (2014)