

https://dspace.org/

Bamboozled: an investigation into systematic regulatory failure in crypto-Ponzi investment schemes, and consumer detriment, in Uganda : a case study of Dunamiscoins Resources Limited

Kafeero, Stephen

2021
https://hdl.handle.net/10539/36690

Downloaded from a DSpace repository. https://dspace.org/



Bamboozled: An investigation into systematic regulatory failure in crypto-Ponzi investment schemes, and consumer detriment, in Uganda.

A case study of Dunamiscoins Resources Limited

Research Report

In Partial Fulfillment of the Requirements

For the Degree of

MASTER OF ARTS (JOURNALISM AND MEDIA STUDIES)

UNIVERSITY OF THE WITWATERSRAND

STUDENT NAME: Stephen Kafeero

STUDENT NUMBER: 2413461

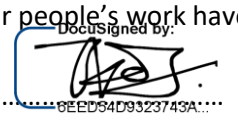
SUPERVISOR: Prof. Anton Harber

“Move in space with minimum waste and maximum joy.”

Sade Adu

Declaration

I, **Stephen Kafeero**, do hereby affirm that this investigative research report is my original work and that it has never been presented to another University or institution for the award of any academic qualification. Statements attributable and or sourced from other people's work have been duly acknowledged.

Signed……

Date…4/16/2021

Stephen Kafeero

Dedication

To my mother, **Winfred Namata**, (1964-1999). Your memory intoxicates me. I want more. I want to make you proud.

Acknowledgment

I am forever indebted to the Open Society Foundation for the scholarship. Indeed, it takes a village! Special thanks to my dream maker and our kind MA coordinator, Prof. Lesley Cowling. I don't take her belief in me for granted. She is a living embodiment that "love recognises no barriers, jumps hurdles, leaps fences, and penetrates walls to arrive at its destination full of hope".

I am eternally grateful to Prof. Anton Harber who inspired me, supported me as I conceived this investigation research project. Endless thanks for his supervision and mentorship. This investigation would not exist without his reliable feedback, guidance and generosity despite the prevailing conditions. The Covid-19 pandemic lost.

I am grateful to the hardworking faculty and staff at the Wits University department of journalism led by Prof. Franz Kruger. Our interaction may have been limited due to the pandemic but those few moments when he and the rest of the team reached out meant a lot to my scared and sometimes confused self.

Special thanks to all the interviewees (sources) who took time off their busy schedules to share their stories, insight, pointers and knowledge during the investigation. To my mother's little sister, Teddy Mutesi, thank you for never walking away. Grateful to Muthoki Mumo, Lydia Namubiru and Gaaki Kigambo. An awesome trio. To the rest of my family and friends, I don't take you for granted. "Life," says Erich Maria Remarque "did not intend to make us perfect. Whoever is perfect belongs in a museum."

List of Acronyms and Abbreviations

DLT……Distributed Ledger Technologies

FSCA……..Financial Services Conduct Authority

NCR……National Credit Regulator

The Hawks…… The Directorate for Priority Crime Investigations

FIC…… Financial Intelligence Centre

KYC…….Know Your Customer

VFA…….Virtual Financial Assets Act

MFSA……..Malta Financial Services Authority

CMA…….Capital Markets Authority

'COWE…….Caring for Orphans, Widows and the Elderly

UMRA……..Uganda Microfinance Regulatory Authority

URSB……Uganda Registration Services Bureau

FIA……Financial Intelligence Authority

BoU……..Bank of Uganda

UCC……...Uganda Communications Commission

EAC……..East African Community

ISO……Internal Security Organisation

UBA…… Uganda Bankers' Association

STRs…… Suspicious Transaction Reports

ICIJ……International Consortium of Investigative Journalists

OSF……Open Society Foundation

Table of Contents

Declaration ..... **Error! Bookmark not defined.**
Dedication ii
Acknowledgment iii
List of Acronyms and Abbreviations iv
Table of Contents v
Abstract vi
Introduction and rationale 1
Cryptocurrency and Blockchain 3
Methodology 4
Hypothesis 5
The case of Dunamiscoins Resources Limited 5
SOURCE MAP 6
Timeline 8
Timeline illustrated 9
Narrative 9
Literature review 10
Uganda's legal and regulatory framework 12
The case of Malta 13
Consumer protection 14
Media coverage 15
The case of COWE 15
Global Cryptocurrencies Ltd 16
Limitations/Ethical issues 17
Authorities, banks in regulatory limbo as crypto-Ponzi schemes destroy dreams and lives 19
Overview of crypto-Ponzi schemes and how to spot them 38
Reflective Essay 39
References 43

Abstract

Financial services are key to Uganda's development. The financial sector is a major contributor to Uganda's public finances, driving the distribution of the country's vital public services. Regulators and other players such as commercial banks in the sector have a responsibility to espouse the highest values of scrupulousness, transparency and accountability to customers and everyone who may be affected by their actions and inactions. Financial regulators have an added responsibility to ensure that the users of the services they oversee are treated fairly and have sufficient information to make informed decisions.

In Uganda, the last four years have instead seen pile-up of crypto-related scandals exacerbated by regulatory failure. There has been abdication of responsibility by legislators, a host of institutions established to regulate the market and other players in the market.

Customers and investors who have pegged their livelihood and expectations of a secure financial future have been left at the hands of get-rich-quick schemes and frauds worsened by financial institutions bent on making a profit and regulators who are either reluctant or lack the necessary tools such as regulations to exercise their mandate.

The rise in crypto-Ponzi schemes in Uganda has demonstrated the fragility and in some cases absence of a corporate and regulatory regime and the weakness of legal means of minimising risk and highlighting dangers of the schemes to the public.

Bamboozled: An investigation into systematic regulatory failure in Crypto-Ponzi investment schemes, and consumer detriment, in Uganda provides an in-depth account of the upsurge of crypto related Ponzi schemes in Uganda and the actions of supervisors, regulators, and bankers with a particular focus on Dunamiscoins Resources Limited**.**

Crypto-Ponzi schemes in the country have been ruinous for businesses, individuals, communities and the Ugandan state adding on the already devastating poverty statistics and suffering. This investigation uncovers the supervisory failure and brings urgent attention to the confusion and ineptitude upon which the crypto-Ponzi schemes thrive.

Introduction and rationale

This investigation is borne out of a recognition that Uganda is in the process of deepening financial inclusion for everyone. This includes the adoption and integration of technology in products offered by financial services entities to create new products and markets as part of a broader strategy to boost their growth (Allmen et al, 2020). Opportunists and self-seekers are, however, taking advantage of this situation by duping the unsuspecting public into schemes that promise them massive profits and new opportunities. The charm of easy cash has seen more and more expectant people unsuspectingly risk their savings or borrowing to invest in schemes that quickly go bust. Thus, this investigation details a litany of failures and devastations of crypto-Ponzi scandals in Uganda and the inquiries focus on the failure of financial regulators and bankers. The findings show that managers of the schemes fattened their accounts while businesses, communities and families were left clutching life-time losses and convulsing in agony. The questionable success of the crypto-Ponzi schemes appear to illuminate failure of the regulators who, all too often, acted with indifference and apparent incompetence.

Uganda's socioeconomic context appeals to Ponzi schemes. The country's population is very young. Eight out of ten people are below the age of 30. The country's national unemployment rate stands at 9.2% while the unemployment rate for youth below 30 is at 13.3%. Other factors such as underemployment, non-rewarding work compel the population to work in jobs that do not offer decent incomes (Among & Munavu, 2019).

This mix is a ripe market for scammers to initiate wealth promising schemes. From 2007 to-date, Uganda is filled with speculation of huge earnings from the crypto currencies. While many Ugandans are gripped by the promise of the rewards from crypto currencies, very few have access or even understand how the technology works. This is the gap that companies like Dunamiscoins Resources exploit, promising a windfall to enthusiasts who invest in crypto currencies. This project aims at investigating and narrating in detail the role of government agencies and their actions or inactions that allow this situation to thrive with a view of bringing urgent attention to the scandalous issues and prevent the same from happening again. It is my belief that unearthing information about schemes such as Dumamiscoins beyond general news reporting creates awareness within the general public, provides information to guide policy formulation and regulation. In addition, such expose makes it harder for the perpetrators and their co-conspirators to target and or exploit more victims.

Ponzi scheme fraudsters are leveraging the latest technology and using the internet to mask or lend credibility to their schemes and dupe investors into putting their money in their scams. Given the limited information available on new or latest technology, potential investors do not have much information to guide their decision making. The emergence of virtual currencies such as Bitcoin have availed fraudsters an opportunity to dupe potential investors to trade on online exchanges for conventional currencies backed by sham or fictitious investments and transactions. Fraudsters behind the Ponzi schemes exploit the internet knowledge gap but also new and exciting technologies such as crypto currency to create an illusion of massive profits for a desperate and ignorant population in search of a better life than they already have or simply looking to amass more wealth (Morris, 2017).

Ponzi schemes employ a trick of picking money from one client or investor and giving it to another person until they run out of new investors or simply when the fraudsters disappear or are compelled to conclude the scheme by authorities. In a Ponzi investment scheme, investors are rewarded high returns from their own money or the money paid by other investors instead of relying on profit earned from the 'investments' which don't exist. The term Ponzi is derived from an Italian crook, Charles Ponzi, who in a period of eight months in the 1920s stole an estimated $15 million from more than 10 thousand people in Boston, United States of America, by simply letting them in on a secret to wealth he had unlocked. Before the Ponzi name was adopted, the schemes basically went with the name that explained them easily "Robbing Peter to pay Paul" (Darby, 1998).

In 2019, at least $4.3 billion was lost to crypto-Ponzi scammers, which was more than double (around $1.7 billion) what had been scammed in 2018 (Akshay, 2020). The proceeds ended up in the hands of a small, but powerful, section of criminals. Scams were the most lucrative class of crypto crime in 2019. Criminals take advantage of the exclusive position cryptocurrency presently enjoys in many societies. It has been marketed as a scheme in which an investor can get rich very quickly. Many people don't understand the trade well enough to spot a crypto-Ponzi scheme when they see one, making them apt targets. Such crypto-Ponzi schemes tend to target vulnerable populations such as the elderly and young people. Scammers promise massive returns for those who invest in their fraudulent schemes, persuading potential victims to invest considerable sums in the hopes of a big payout. Scammers typically promote themselves aggressively in the media and elsewhere, including building sophisticated websites (Akshay, 2020).

In Uganda, avenues of duping and stealing from unsuspecting members of the public are rapidly evolving. They range from job scams where the victim is promised a job and conned through application and validation fees, hacking of social media accounts where friends and relatives of a victim are duped into sending money to help their own, impersonation of famous people to email and mobile money fraud (Kimbowa, 2018). In the last 15 years, from 2005, at least 20 Ponzi schemes have been successfully executed in Uganda fleecing thousands of Ugandans of billions of shillings (Kazibwe, 2019).

Crypto-Ponzi schemes rely on a similar design as the traditional Ponzi schemes. Scammers appeal to people's desire for quick profit and promise them high returns on their investment within a short time. It follows, therefore, that the first group of investors get paid, which habitually entices more people. Fraudsters are using new technologies such as virtual currencies to execute their schemes because transactions in virtual currencies apparently have greater confidentiality benefits and less regulatory oversight than dealings in conventional currencies (Akshay, 2020). While cryptocurrencies were developed and touted as an alternative payment system to traditional currencies, they have evolved and are now traded and marketed as a highly speculative investment chattels and assets. Countries have taken differing approaches to cryptocurrencies. For instance, China and Vietnam have opted for outright bans, Japan and the United Kingdom have embraced them and the United States has chosen to monitor pending a final decision. As Masie (2018) argues, there is no protection in developing countries for investors in cryptocurrencies.

Cryptocurrency and Blockchain

A cryptocurrency is a digital asset formulated to work as a medium of exchange. It relies on cryptography for security. Many cryptocurrencies are decentralised systems based on blockchain technology, a distributed ledger technology (DLT) enforced by a distributed network of computers. A crucial feature of a cryptocurrency, and debatably its chief attraction to both scammers and legitimate users, is its organic nature; it is not issued by any central power, making it hypothetically invulnerable to government interference or manipulation (Rosic, 2016).

A blockchain is plainly just a chain of blocks, where in this context, the words "block" and "chain" refer to digital data (the "block") stored in a public database (the "chain"). The digital information is recorded in a database and is distributed over a vast network of computers. Because blockchain enables for digital information to be securely stored and transferred

directly from one party to another, valuable digital information also known as digital assets can be exchanged electronically, and one of these digital assets are cryptocurrencies. Therefore, the relationship between blockchain and cryptocurrencies is that cryptocurrencies form part of blockchain technology. Aside from cryptocurrencies, the applications of blockchain technology are vast, and are being tested in various fields which are hinged on the storage or exchange of valuable information or trust. This includes the legal field, the logistics industry, identity services, payment systems, cybersecurity and many others (Hall, 2018).

Crypto-Ponzi are essentially fraudulent investment schemes that may involve cryptocurrencies such as Bitcoin or are clothed under such virtual currencies. Those behind Crypto-Ponzi often recruit new investors by promising to invest cryptocurrencies claimed to generate high returns with little or no risk. Like in traditional Ponzi schemes, the fraudulent players focus on bringing in new money to fund payments already promised to other investors and to make their cut. Crypto-Ponzi schemes have been successful largely because cryptocurrencies are a new innovation, technology that many people including financial regulators are still learning about. What distinguishes Crypto-Ponzi from a regular Ponzi scheme is the idea on which it is based (Supra, 2018). In a classic crypto-Ponzi scheme case of SEC v. Shavers, in the United States, the organiser of an alleged Ponzi scheme advertised a Bitcoin "investment opportunity" in an online Bitcoin forum. Investors were allegedly promised up to 7% interest per week and that the invested funds would be used for Bitcoin arbitrage activities in order to generate the returns. Instead, invested Bitcoins were allegedly used to pay existing investors and exchanged into US dollars to pay the organiser's personal expenses (SEC, 2013).

Methodology

This investigation uses the hypothesis-based inquiry, sometimes referred to as the story-based inquiry. This method involves four aspects including translating a question into a hypothesis, developing a timeline, mapping the stakeholders and creating a Masterfile, basically a data base, from which the final piece of the investigation is drawn and written(Hunter, 2011). Investigative Journalism involves looking into dark places and unveiling of matters through questioning and probing which culminates into the examination and exposure of all pertinent facts to the public (Harber, 2018). The story based inquiry method aids this process of investigative journalism described above by using stories as the interconnection of every step of the investigation process from conception to research, writing, quality control and even publication. Story-Based Inquiry developed by Mark Lee Hunter involves researching and writing investigations as one integrated process. It will begin with a hypothesis, a draft story

that will define and guides the investigation. A timeline and source map will identify what is under investigation and where to find it. A master file will keep the investigation focused, and will act as the pillar for the finished narrative, and provide a database for future projects (Hunter, 2011). The orderly approach of this method will allow the journalist to collect the data, organise it so that it is easier to examine, compose into a story, and check. Further, it will allow assembling of documents and other material evidence such as clips for easy retrieval. This elaborate procedure enables identification of gaps in the investigation. The hypothesis, as Sengers & Hunter (2012) argue, contains news, a basis, and a resolution to keep focus on both the facts and the story. In this way, hypothesis is either verified or disproved.

The timelines will guide the journalist by allowing them to see what happened including between known events, and how they concluded. The journalist will be able to focus on dramatic scenes that will deepen the impact of their work and possible structure for their narrative. In creating the source map, the journalist will be able to track the characters and subjects of the investigation including experts, actors, victims and witnesses. By linking the relationship of the sources, the journalist will be able to spot more sources involved. Finally, the journalist will move what is captured in the Master File, a data base of all the material the journalist requires for analysis to make the final investigation report. Overall, the method will allow the journalist to create clarity on the significance of the investigation by asking such questions around the number of people affected, the magnitude of the impact, whether positive or negative, those culpable for wrongdoing if any(Hunter, 2011).

Hypothesis

Regulatory and supervisory failures by state agencies allows crypto-Ponzi schemes to defraud Ugandans.

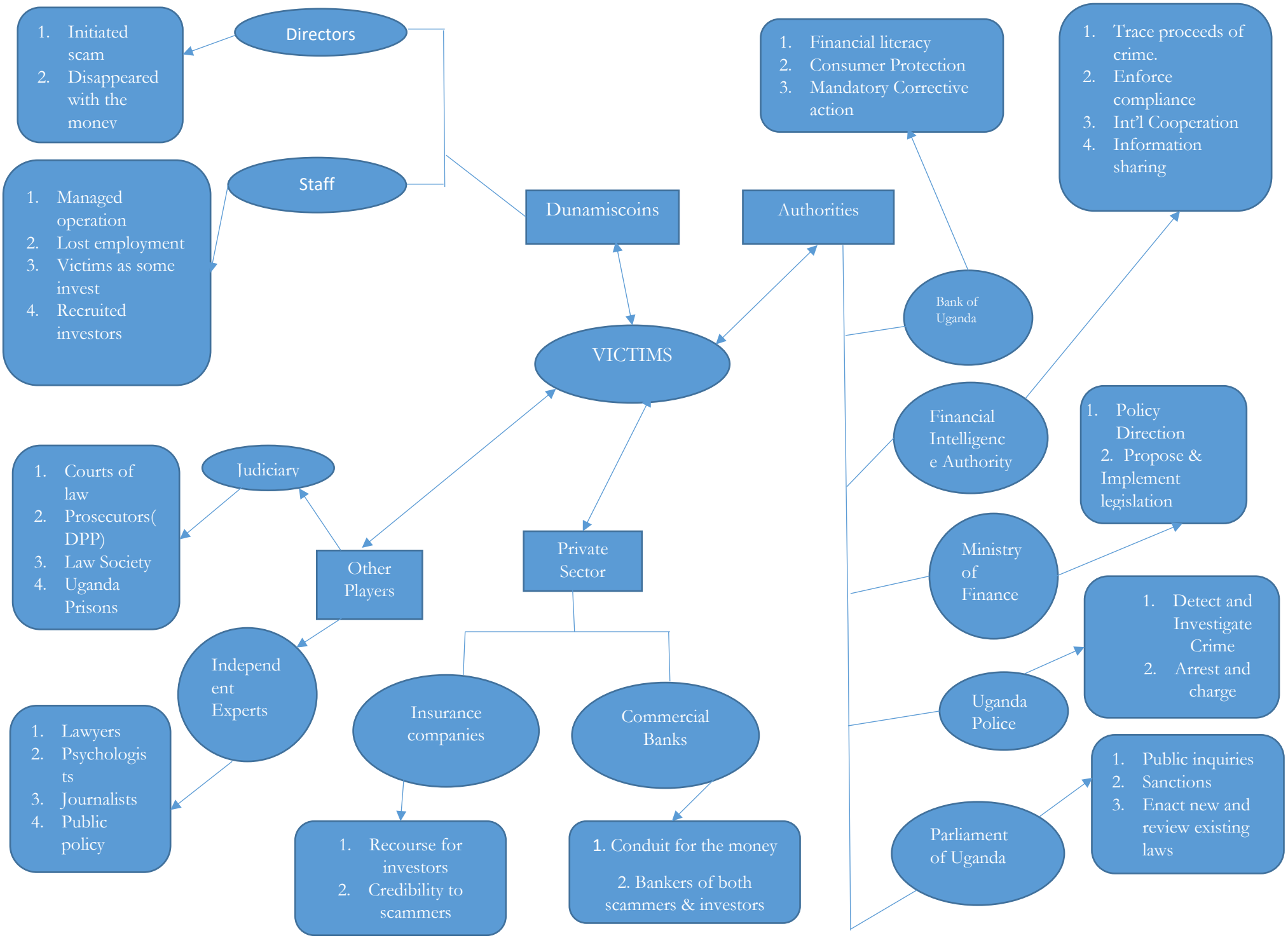
The case of Dunamiscoins Resources Limited

Dunamiscoins Resources Limited was registered under the laws of Uganda (80020001481676) on January 21, 2019, as a private company limited by shares. It operated legally within the country's financial system with known head offices on Plot 11A Rotary Avenue in Uganda's capital, Kampala. Out of the blue in December 2019, both customers and staff woke up to a rude shock that the company was broke. The staff could not make the daily payments and the customers could not receive their money which was due. Dunamiscoins is reported to have defrauded 2,500 people of UGX20 billion or US$5.3m. Each of the depositors was promised a 40 percent interest on their deposits after 21 working days. The early investors benefitted and

received the promised 40 percent interest on their investments. By November 2019, the company increased interest to 50% on each deposit. A month later, branches started running out of cash and could not meet the daily demands of the customers and as such began shutting down. The Directors were reported to have disappeared. At least UGX47m or US$12,554 was recovered from Dunamiscoins Resources Ltd branches while UGX 709m or US$189,389 was frozen on their accounts. Police and other authorities launched investigations and two suspects, both Ugandans; Nabunya Mary and Lwanga Simon, were arrested and charged at the Law Development Center court (vide Old Kampala CRB 1577/2019), and sent on remand (Kamusiime & Isah, 2020).

SOURCE MAP

The Source Map below will guide the investigation in examining the validity of the study hypothesis. The elements in the source map piece the links in unravelling parties involved and what happened. Source mapping entails identifying who the key actors in the story are and any documents that record their actions. The various sources identified will help in proving or disproving the investigation's original hypothesis. For every detail, the investigation will rely on a two-source principle, which implies the journalist will use at least two independent sources to ascertain the same information. This journalist has constructed a mind-map below to help ease the process of finding the sources needed for the investigation. This process will help the journalist to create a sequence of events that describes events such as dates and places (Nazakat, 2017).

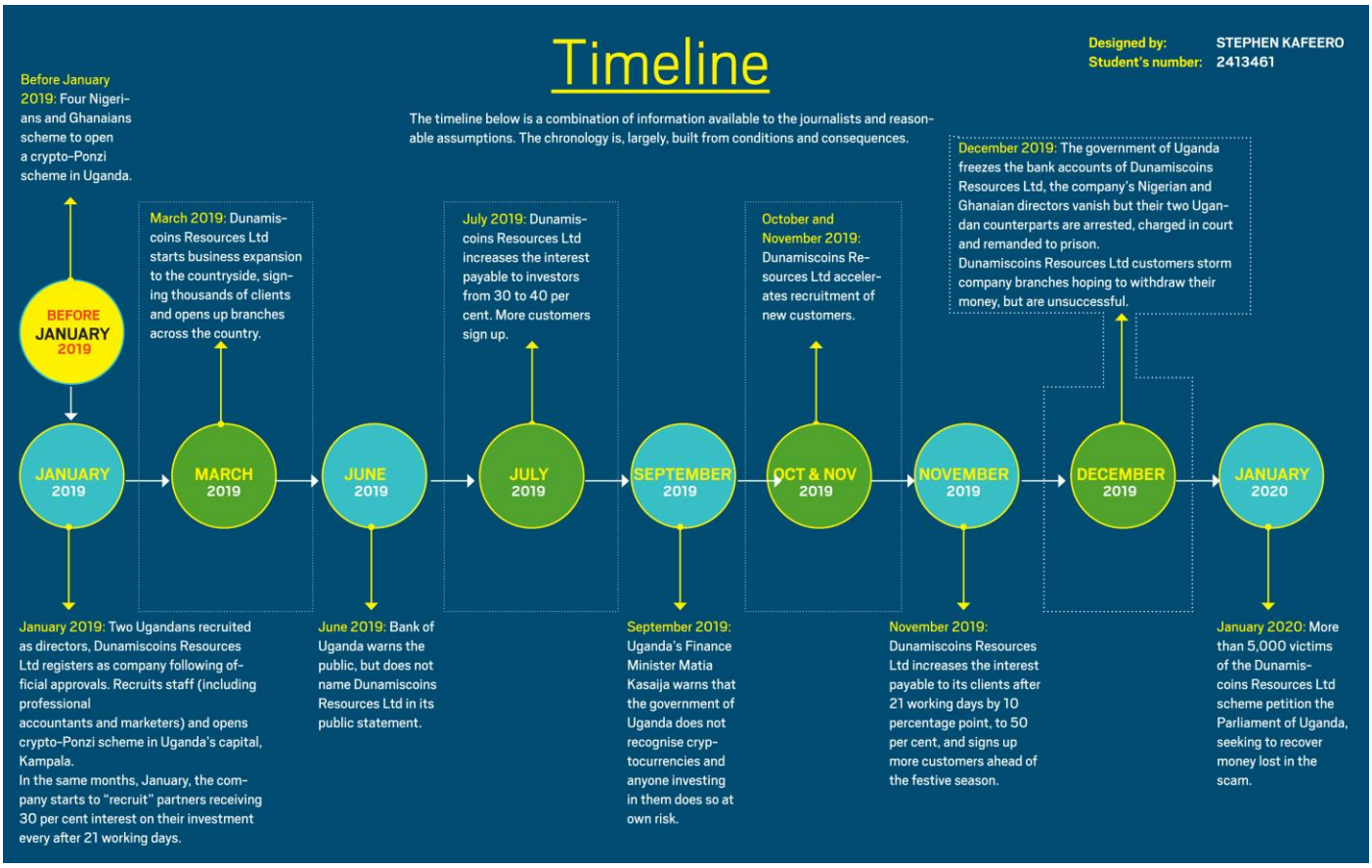

1. Initiated scam
2. Disappeared with the money
Directors
Staff
1. Managed operation
2. Lost employment
3. Victims as some invest
4. Recruited investors
Dunamiscoins
VICTIMS
Authorities
1. Financial literacy
2. Consumer Protection
3. Mandatory Corrective action
1. Trace proceeds of crime.
2. Enforce compliance
3. Int'l Cooperation
4. Information sharing
Bank of Uganda
Financial Intelligence Authority
1. Policy Direction
2. Propose & Implement legislation
Ministry of Finance
1. Courts of law
2. Prosecutors(DPP)
3. Law Society
4. Uganda Prisons
Judiciary
Other Players
Private Sector
Independent Experts
1. Lawyers
2. Psychologists
3. Journalists
4. Public policy
Insurance companies
Commercial Banks
1. Recourse for investors
2. Credibility to scammers
1. Conduit for the money
2. Bankers of both scammers & investors
1. Detect and Investigate Crime
2. Arrest and charge
Uganda Police
Parliament of Uganda
1. Public inquiries
2. Sanctions
3. Enact new and review existing laws

Timeline

The timeline below is a combination of information available to the journalists and reasonable assumptions. The chronology is, largely, built from conditions and consequences.

1. Before January 2019: Four Nigerians and Ghanaians scheme to open a crypto-Ponzi scheme in Uganda.
2. January 2019: Two Ugandans recruited as directors, Dunamiscoins Resources Ltd registers as company following official approvals.
3. Recruits staff (including professional accountants and marketers) and opens crypto-Ponzi scheme in Uganda's capital, Kampala.
4. In the same months, January, the company starts to "recruit" partners receiving 30 per cent interest on their investment every after 21 working days.
5. March 2019: Dunamiscoins Resources Ltd starts business expansion to the countryside, signing thousands of clients and opens up branches across the country.
6. June 2019: Bank of Uganda warns the public, but does not name Dunamiscoins Resources Ltd in its public statement.
7. July 2019: Dunamiscoins Resources Ltd increases the interest payable to investors from 30 to 40 per cent. More customers sign up.
8. September 2019: Uganda's Finance Minister Matia Kasaija warns that the government of Uganda does not recognise cryptocurrencies and anyone investing in them does so at own risk.
9. October and November 2019: Dunamiscoins Resources Ltd accelerates recruitment of new customers.
10. November 2019: Dunamiscoins Resources Ltd increases the interest payable to its clients after 21 working days by 10 percentage point, to 50 per cent, and signs up more customers ahead of the festive season.
11. December 2019: The government of Uganda freezes the bank accounts of Dunamiscoins Resources Ltd, the company's Nigerian and Ghanaian directors vanish but their two Ugandan counterparts are arrested, charged in court and remanded to prison.
12. Dunamiscoins Resources Ltd customers storm company branches hoping to withdraw their money, but are unsuccessful.
13. January 2020: More than 5,000 victims of the Dunamiscoins Resources Ltd scheme petition the Parliament of Uganda, seeking to recover money lost in the scam.

Timeline illustrated



Narrative

For decades, Ponzi schemes have been hatched and executed in Uganda (Kazibwe, 2019). A new trend, however, has emerged with scammers putting a high-tech spin on the old-fashioned Ponzi schemes through new technology such as cryptocurrencies. Current reportage on the old-fashioned Ponzi schemes and the new digital schemes have focused more on the events such as the closure of the schemes and victims' agony and struggles to recover lost money. Blame has been levied on the victims by both the both officials of the government of Uganda and the general population while regulators take refuge behind general notices to the public, warning about Ponzi schemes. To-date, there is no investigation in the role of the government agencies in the success and failure of the crypto-Ponzi schemes.

This investigation examines the disaster of crypto-Ponzi schemes in Uganda by spotlighting institutional and regulatory failures by Uganda government as well as corporate

mismanagement. Besides human sources, the journalist in executing this inquiry uncovers documentary evidence, examines laws establishing or guiding the work of the relevant government agencies, sifts through police investigation reports and documentation about Dunamiscoins Resources Ltd and other Ponzi schemes as well as analyses official banks' correspondences. This approach provides the background, the context and the detailed information needed to ask more probing questions from sources.

Sourcing of the story includes conducting interview with Dunamiscoins Resources Ltd owners and staff, regulators, victims, investigators, officials of banks and government agencies and other experts to establish what happened and obtain information beyond what the documents provide, including anecdotal evidence.

The internet and other electronic records aid the investigation as secondary. A search and analysis of information in computer databases about various Ponzi schemes enables observations and comparison of trends and patterns regarding operations, collapse and Ponzi schemes' investigations. An examination of the relevant laws is to illuminate the roles, powers and mandates of key agencies and their application – or the lack thereof – in relation to Dunamiscoins Resources Ltd, and why. The journalist will follow the money which will inform the investigation on regulators' actions and inactions. The question of money is central to the investigation in the sense that all the schemes are set up to fraudulently obtain money. The money trail is ascertained by examining how the money was obtained, processed and kept and the parties involved in that process until the collapse of Dunamiscoins Resources Ltd. Further, important questions this investigation asks, and answers, include the whereabouts of the missing money of Dunamiscoins Resources Ltd clients. If it was taken out of the banks or Uganda, how was this done and by who? Were proper and established procedures followed? Did it raise any alarm from the regulators, for example, Bank of Uganda and Financial Intelligence Authority? If yes, did they take any timely action and, if so, what actions? If no, why? What information was available to the various agencies and clients about the Dunamiscoins Resources Ltd? If the regulators were caught off-guard, at what point did they know, how and what tools were available to them for action?

5. Literature review

No legal system is immune to Ponzi schemes, but the extent of their occurrence and impact is mitigated by a proactive regulatory regime in a specific jurisdiction especially if they are made a top priority. Suspected cases are quickly publicized and authorities move fast against the

entities and individuals involved by indicting and prosecuting them. Emerging financial systems, however, lack sector specific regulations and agencies which are empowered with the required resources to execute their mandate to react quickly and efficiently to protect the potential victims. In instances where the scammers are successful, the systems within these jurisdictions lack the skills and resources to initiate and sustain proceedings against the perpetrators as a means of recovering. The situation is made worse by the relatively low levels of literacy within the population which makes it more vulnerable. Battling Ponzi schemes goes beyond the conventional branches of the law and requires overhauling or creation of specialised entities, financial regulations with staff equipped with adequate expertise. Education of the investing public is a must as a mitigating factor (Tajti, 2019).

Some of the biggest Ponzi schemes happen under the radar of the authorities yet they do nothing to stop them until it is too late, which raises concerns of possible collusion or incompetence of the regulators. A money-spinning South African "investment scheme", Bitcoin Wallet, which went under in July 2009 was well known to authorities and recruited its victims openly. The scheme lured investors with promises of doubling their investment in about two weeks through trading the customer deposits in cryptocurrencies. Within a short time, the firm became so popular that the fraudsters behind it ceased accepting deposits less than 5,000 rand or US $350 (Kuhn, 2019). South Africa's sector regulators, Financial Services Conduct Authority (FSCA) and National Credit Regulator (NCR), claimed Bitcoin Wallet's business certificate was a forgery and needed to be investigated among a string of queries which, if raised earlier, would have protected the investors. Also, the fraudsters often enjoy overt protection by security authorities which clothes then from suspicion or sanction. The Directorate for Priority Crime Investigations (The Hawks) provided police escort to Sphelele "Sgumza" Mbatha, the individual behind Bitcoin Wallet (Ana, 2019).

Some of these officials, usually state employees, use the inside information they have about the viability of the scheme to their advantage by letting the scheme operate. They become investors, but leverage the inside information they have and get out before the scheme collapses. This situation creates two sets of investors - the informed and uninformed. Informed investors have control over information dissemination, law enforcement and use this power to their advantage (Sadiraj & Schram, 2018).

There is evidence that when officials use their authority and act quickly they are able to stop the Ponzi schemes in their infancy and save the would-be victims from being conned. One such

instance is when the Financial Intelligence Centre (FIC), South Africa's national center for collecting and investigating transactional and related information, identified what appeared to be a Ponzi scheme run by an individual marketing a "new crypto currency" in its infancy. The fraudsters marketed their product as Africa's first crypto currency, promising investors massive profits on their respective investments. When FIC combed the individual's bank statements, it was discovered that there was no cryptocurrency and that this was in fact a Ponzi scheme. Consequently, an order was issued on the more than R2.8 million in proceeds from the alleged scheme. A separate order pertaining to fixed property worth more than R4 million purchased using funds obtained from the scheme was obtained (FIC, 2019).

Uganda's legal and regulatory framework

Uganda is yet to enact crypto-currency-specific legislation. However, there is existing legislation that in the least can be considered to be relevant including the Electronic Transactions Act, 2011 and the Electronic Signatures Act, 2011. The Electronic Transactions Act, 2011, generally deals with digital transactions and defines digital signatures to mean a transformation of a message using asymmetric cryptosystem. The relevance and enforceability of these laws to blockchain related matters is hinged on the understanding of the technology prevalent at the time. The current law is designed around a centralized system and yet blockchain by its nature promotes decentralization. Any law in this space needs to be more technologically agnostic (Muhangi, 2020).

In May 2020, the Parliament of Uganda passed the National Payment Systems Bill into law making it a requirement for all persons who are moving value on blockchain platforms including cryptocurrencies to be licensed by Bank of Uganda, the country's central bank, and pay some license fees which are yet to be determined. Businesses engaged in crypto-currency will have, for instance, to state dispute resolution mechanisms and describe the contact persons for their entity, provide for risk management and business continuity procedures (Nakaweesi, 2020). Uganda has also established a National Taskforce on the 4th Industrial Revolution drawn from different spheres of the country's society which is expected to recommend policy interventions and legislation (Masereka, 2019).

Existing financial and tax sector legislation is quiet when it comes to cryptocurrencies except within the anti-money laundering framework which makes companies and their directors accountable persons. While cryptocurrency trading is becoming common in Uganda, regulators of financial institutions have been either dismissive or cautionary. On 30 September, 2019,

Uganda's Minister of Finance Matia Kasaija issued an official statement to the effect that cryptocurrencies are not officially recognized as legal tender in Uganda. Other than the cautionary statements such as the one above, there are no prohibitions on the use or trading of cryptocurrencies in Uganda at this time (The Independent, 2019; Odyek, 2019).

Further, Uganda's Insolvency Act, 2011 is unable to deal with insolvency issues that may arise with crypto-based entities. Recourse for parties engaged in crypto-currency trading and investment is left to the traditional legislation where Anti-Money laundering, Know Your Customer (KYC) and consumer protection requirements governing the banking industry do apply to any companies or other juridical persons dealing in cryptocurrency or other blockchain products. These legislations include: The Financial Institutions Act of 2004 and the attendant regulations under it; the Anti-Money Laundering Act of 2013 (as amended); the Consumer Protection Guidelines of 2012 (written and enforced by the central bank). The Anti-Terrorism Amendment Act of 2015, whose purpose is to address terrorism financing concerns, has a very comprehensive definition of the term funds to include assets of every kind, whether tangible or intangible, movable or immovable, however acquired, legal documents or instruments in any form including electronic or digital, evidencing title to, or interests in such assets. This definition can be purposively interpreted to cover the ownership or movement of cryptocurrencies. It that while there are no express prohibitions to the use of crypto-currencies, Ugandan authorities are alive to the threats and concerns associated with crypto-currencies including crime and fraud. Traditional criminal, commercial and civil law protections and prohibitions under the Penal Code Act, Capital Markets Authority Act, Financial Institutions Act, and the general body of precedent apply (Muhangi, 2020. The case of the Republic of Malta, discussed below, is instructive on specific legislation and best practice for Uganda.

The case of Malta

Countries like Malta that recognize the opportunity that technologies such as cryptocurrency offer have moved to enact specific legislation to stop fraudsters from taking advantage to scam unsuspecting citizens. In 2018, Malta enacted The Virtual Financial Assets Act (The VFA Act), which sets up a regulatory environment and provides legal certainty for individuals and entities wishing to invest providing clarity and enhancing market integrity and transparency. The Act also provides apt guidelines on how collected funds may be spent, and how due diligence on the individuals seeking for funds is to be carried out and, crucially, clarifies that businesses will be liable to pay damages to anyone that loses money due to misrepresentations. The Act,

in summary, establishes a strong compliance and implementation regime in Malta and lays down the necessary fundamentals to strengthen investor protection and limit market abuse (Pisani, 2018). One of the highlights of Malta's VFA Act is the requirement that those who seek funds and to engage in the sector register a "White Paper" with the Malta Financial Services Authority (MFSA), which is responsible for supervision and enforcing its provisions. The white paper must include: the motive of the initial offering, description of the platform and its benefits, how it will be sustained, the risks, and extenuating procedures of the offering, the characteristics of the financial assets offered, and a description of the issuer (Feikert-Ahalt, 2019).

Consumer protection

Legislation and regulation pertaining consumer protection in Uganda is disjointed. Over the years, fragmented legal dispensation has taken center stage with the laws and their practical implementation at variance. The degree of consumer protection has a positive impact on the level of development and Uganda needs to overhaul of the current legal framework and put in place a comprehensive consumer protection legislation (Zeija, 2018).

Bank of Uganda working with financial institutions under the central bank's supervision such as commercial banks in the country has a three-pronged strategy for financial consumer protection. This involves increasing the awareness of consumers, strengthening the central bank's supervisory techniques to ensure compliance and working with the supervised institutions to ensure a clear understanding of what is required.

This entails development of documents with key information on savings and loans products, training the supervised financial institutions, improving on the complaints handling procedure, strengthening the central bank supervision of compliance with its rules especially on consumer protection (BOU, 2011). Consumers or investors have a duty imposed on them by the Uganda's Capital Markets Authority (CMA) which largely deals with investor to be careful of the decisions they take in buying and selling of securities. Before making a trade or investing in a scheme, investors are required to seek adequate investment advice from licensed intermediaries.

Financial reegulators like Bank of Uganda, Uganda's central bank, have specific mandates for protecting consumers. For example, the central bank has a mandate of supervising financial institutions derived from the Financial Institutions Act 2004, the Micro-Deposit Taking Institutions Act 2003 and the Bank of Uganda Act 1993. The aim of this to ensure a safe and

sound financial system that protects depositors funds and conducive for macro-economic stability.

Media coverage

Uganda's media sector is diverse with more than 300 licensed radio stations and 30 (free to air) TV stations. These serve close to 40 million people with radio remaining the dominant medium. More than three-quarters of the population own a mobile phone with less than 16% of these smart phones (BBC, 2019). Much of the coverage of the unfolding crypto-Ponzi scandal in Uganda has been event based. A review of the coverage in print, broadcast and social media prior to the collapse of Dunamiscoins and other schemes and post their collapse shows the media focused on the events. The stories focused on the suspects arrested and charged in court, the grievances of the victims and the views of the authorities. In-depth reporting and attempts at investigating are occurring much later and in some cases based on police reports (Bagala, 2020).

1. **Impact on victims**

This section briefly reviews some of the crypto-Ponzi schemes that have been orchestrated in Uganda and cites a case of one of the many other Ponzi schemes to create understanding of the impact on the victims.

The case of COWE

Starting 2007, conmen operating under the cover of a non-profit organization, 'Caring for Orphans, Widows and the Elderly,' (COWE) defrauded unsuspecting Ugandans, mainly the elderly and poor women in villages, of billions of shillings. The trick was to ask them to invest and receive high returns from donors who would rely on the victim's demonstrated commitment to help them fight poverty. The organization held a NGO license, but operated as a bank or microfinance institution and held marketing campaigns across the country including radio adverts. More than 3,000 people invested by mortgaging their property like land to banks to cash in on the astronomical 54 per cent profit promised. State authorities including Uganda's central bank were aware of the crypto-Ponzi schemes in the country including Dunamiscoins and made general warnings to the public. Beyond the warnings, there is no information to suggest that they made effort to crackdown on any of the schemes until the schemes collapsed.

In 2006, Uganda's central bank or Bank of Uganda, as it is formally called, had tried to intervene by freezing the organisation's account but the fraudsters successfully challenged this

move in the High Court by claiming they had not been given a fair hearing. This gave them an opportunity to clean the accounts and disappear. A decision by the appeals court three years later, in 2009, was too late (Kavuma, 2016). Many of the victims reported to the police, but COWE directors were never brought to justice. Ten years later after the scheme was started, at least four victims had killed themselves with their suicides directly linked to the scam. Worse, many of the victims have been incarcerated over loans they failed to repay to commercial banks and microfinance entities (Kushaba, 2016).

Global Cryptocurrencies Ltd

This crypto-Ponzi scheme reportedly stole UGX 10.6BN from at least 425 people according to police reports and court documents. The victims included senior military and police personnel who borrowed from other sources including banks to take advantage of the 40 per cent profits promised by the scammers. Investors were promised an interest of 40% after registering with their national ID, driver's license, employment ID or passport and would deposit their investments in Stanbic and Centenary Banks, two major commercial banks in the country. For more than a year, between 2018 (when the scheme started) to 2019, the investors were duly paid their investment and interest for every month and this compelled many to invest further and with larger sums. The scam generated UGX900 million per day in investments (Kazibwe, 2019).

One Coin

Ugandans were among the victims of the global crypto-Ponzi scam OneCoin orchestrated by Ruja Ignatova aka Crypto-queen who marketed her scheme as an invention of a cryptocurrency to rival Bitcoin before persuading people to invest. She disappeared. There is no data to indicate how much Ugandans lost as part of the US$5.2 to US$16 billion lost to the OneCoin crypto-Ponzi scam between August 2014 and March 2017 which targeted congregants in Pentecostal churches and rural areas (Bartlett, 2019).

Multimedia

For this investigative project, the journalists envisages a high quality explanatory audio-visual package to fulfil the multimedia requirement of the project. The journalist will extract themes, findings and other interesting ideas of the project and using the skills and experience gained in the other aspects of this course, convert them into a short explainer video that educates and

creates further understanding of the key aspects of the investigation. Infographics such as charts and graphs will also be incorporated in the writing and presentation of the information.

Reflective Essay

This part captures the journalist's critical examination of the investigative reporting project and the attendant life experience. A reflective essay, in this context, involves the journalist writing about the process, attitude, impression or idea regarding the investigation and how it informed their personal experience and growth (Fensham, 1985). The journalist will create a database with signpost questions that will be raised and answered during the process of this investigation and this will inform the reflective essay. The signpost questions will, for example, rotate on themes such as what the journalist learned as a result of the experience, personal development during the process, the impact (positive and negative), the choices made by the journalist and with hindsight what could be changed and maintained.

6. Limitations/Ethical issues

Traditionally, journalistic investigation is treated as operating outside the purview of the requirement of ethics clearances given the prevailing debates on its status as research and the hesitancy of practitioners of journalism to subject their investigations to committee evaluation. Beasley & Walker (2014) argue that there are challenges of journalistic research related to the interview and other clashes of culture between journalistic research, the fourth estate function of journalism and ethics committees that also have an impact on the willingness of researchers to submit their work and the ability of the committees to advise effectively on that work.

Davies, 2011 (cited in ibid), observes that the requirement to submit questions prior, to stick these questions and to amend the questions, where required, in order to protect the vulnerable and those at risk is often at variance with the functions of journalism. Journalistic investigation entails networking and interactions with human sources that may be impromptu, unplanned for safety purposes and may not resemble the type of formal interviews that fall under the scope of the ethics committee (Richards, 2010). It is, however, understandable that Ethics Committee's demands are, therefore, hinged on minimising the harm on any of the participants in the research which implies a level of 'informed consent' while the ethical starting point for journalists is minimising the harm that might be caused to the wider community which is usually marketed as public interest (Dickinson, 2019). As a solution, it is argued that the requirement for formal letters duly double-signed by interviewees and the waver of informed

consent are necessary if the research can be proven to expose unlawful acts or corrupt behaviour and if a 'greater social good results from the exposure'. Such amendments allow journalistic research to investigate areas in a safer and more reliable manner than when all participants are required to be notified and to give permission for inclusion (Beasley & Walker, 2014). This investigation project considers ethical issues underpinning journalistic research. Given that the investigation relies on interviews and case study approaches, both of which involve human participants, it is imperative to adhere to the ethics guiding this research method as Alshenqeeti (2014) argues. The University of the Witwatersrand requires that ethics clearance be obtained by students who are doing research where participants are human subjects. Students are barred from commencing data collection without having an ethics clearance and protocol number issued (University of the Witwatersrand, 2020). Ethical clearance will be applied for from the University.

This investigation project will involve interviewing vulnerable groups, for example, the victims of the crypto-Ponzi scams. To that end, an interviewee accepting to be interviewed, it will be considered that the interviewee has consented to share, and have published, any information they make available to the interviewer. Sources (participants) will be informed at the outset of the purpose and scope of the study, the types of questions likely to be asked and so forth. The journalist will also disclose to the participants their professional background in a manner illuminated by Allmark et al (2009). This investigation is happening amid the COVID-19 pandemic and its attendant restrictions including lockdowns and bans on travel and physical interactions which challenge the ability of researchers including journalists to collect primary data. The news gathering process has traditionally created opportunity for journalists to interface in-person with sources, either through personal appointments or spontaneously, build rapport and trust that enables less-constrained sharing of information, even sensitive information. However, the journalist plans to significantly rely on electronic platforms such as email, social networks (Facebook, Twitter, WhatsApp, and Zoom) and media sharing sites (YouTube) to correspond with, and obtain information, sources. (Greeff, 2020) cautions that this requires 'more effort, time and creativity' and poses challenges such as 'decreased non-verbal signaling' but can be implemented and is doable.

Authorities, banks in regulatory limbo as crypto-Ponzi schemes destroy dreams and lives

Regulators and commercial banks in Uganda knew about a crypto-Ponzi scheme that defrauded investors of billions of shillings, but took no action to protect clients until it was too late, this investigation reveals.

A review of documents obtained during investigations, alongside interviews with the victims, confidential sources, experts and officials of banks and state agencies, suggest widespread systemic and institutional failures where government officials for unexplained reasons were unable to execute their legal mandates.

Behind the latest crypto-Ponzi scam is Dunamiscoins Resources Ltd, a company that Nigerian and Ghanaian nationals founded in Uganda in 2019. The firm had four local directors, Nabunnya Mary, Lwanga Samson, Susan Awon and Makula Faith and enlisted thousands of Ugandans as customers, who in turn injected billions of shillings, before the establishment suddenly went bust within a year of opening business.

The investigations also reveal how majority Dunamiscoins Resources Ltd clients had limited to no understanding of how the virtual currency business runs, and were just eager to cash in on a windfall that the firm promised in up to 50 per cent interest on roughly a month's investment.

This inadequate knowledge about a complicated, technology-driven transaction, as the inquiries found out, from the outset rendered the Crypto-currency dealers vulnerable to exploitation as most of them were either unable or unwilling to do due diligence on the company before committing to invest their money through it.

The case was made worse by an apparent laissez faire approach by Uganda's financial sector regulators, whose laxity appeared replicated down the official chain, creating a dark room in which officials of Dunamiscoins Resources Ltd took cash in rapid succession, and without oversight, from unsuspecting clients.

This was not entirely surprising. Similar Ponzi schemes through which Ugandans have lost billions of shillings have at different times emerged and collapsed in the country, which theoretically would be expected to place both citizens and officials on guard and skeptical about new get-rich-quick schemes.

As the case of Dunamiscoins Resources Ltd shows, it appears no lesson was learnt while all previous scams were either forgotten or ignored in the chase for quick riches.

This investigation found that authorities in Uganda, citing the absence of laws to specifically regulate blockchain technology transactions, simply folded their arms and looked on as Dunamiscoins Resources Ltd ploughed its way to wealth from impoverished citizens.

The Ugandan Parliament, for example, has on several occasions debated and made pronouncements on Ponzi schemes including in 2018, a year prior to the Dunamiscoins Resources Ltd scheme collapse. Neither Parliament's resolutions, which include a November 2018 ban all Ponzi and Pyramid schemes, nor were the promises by the executive to take "action" ever implemented.

Whereas Dunamiscoins Resources Ltd was duly licensed, there is no evidence to suggest that authorities enforced the rules to ensure the company complied with its license terms. Dunamiscoins Resources Ltd, for example, opened and operated branches and ceased operations without the prior written approval of Uganda Microfinance Regulatory Authority (UMRA) contrary to the Tier 4 Microfinance and Money Lenders (Non-Deposit Taking. Microfinance Institutions) Regulations, 2018.

This is crucial because Dunamiscoins Resources Ltd was duly registered by both the Uganda Registration Services Bureau (URSB) and UMRA. The entity was registered as a private limited company incorporated in Uganda whose registration number is 8002000148167.

It is at the UMRA where the scam began to take shape. UMRA established by the section 6 of the Tier 4 Microfinance Institutions and Money Lenders Act, 2016 to license, regulate and supervise Tier 4 Microfinance Institutions and Money Lenders in Uganda. The objective of the regulation, among other things, is to protect consumers of microfinance services against predatory lending and unethical practices aimed at restoring confidence in the microfinance system to promote financial inclusion.

I presented my findings to UMRA and asked them whether they had done the due diligence on the entity prior to registration. "They were licensed to lend money in the form of micro loans," UMRA Executive Director Edith Tusubira said, confirming that the company was properly incorporated.

So, how did UMRA fail to follow up on its licensed entity to ensure it was complying with the requirements of its license? In response to this question, Ms. Tusubira said they unearthed the anomaly during field supervision when they found the company offices closed.

"UMRA carried out an investigation and found out that the customers who allegedly lost money with the company were partners. They were persuaded to buy shares with the company after being promised extraordinary profits. They were promised up to 40 per cent monthly profit not knowing they were being enticed to get into the trap before being defrauded," she says.

"UMRA," she adds, "received complaints from dozens of Dunamiscoins customers but they were advised to seek redress elsewhere because they were not depositors. In fact, they colluded with Dunamiscoins and violated sections of the Tier 4 Act."

I did not find evidence of the said field supervision and UMRA did not provide any despite my insistence. Even if it happened, it was inconsequential given the collapse of Dunamiscoins and closure of their offices was public.

In all the cases reviewed, crypto-Ponzi schemes are registered by the authorities in Uganda and they rely largely on legitimate network marketing.

"Registration is one thing and monitoring of the activities is another because what these people were doing is [that] they were acting beyond the scope of the license given to them by UMRA. You can say they were registered formally, but the activities they were carrying out were not in line with the requirements of their license," says Sydney Asubo, the Executive Director of Uganda's Financial Intelligence Authority (FIA).

Mr. Asubo, the self-styled "Uganda's Chief Hunter of Money Launderers", says the scammers took advantage of a lack of a regulatory framework and lack of awareness about how crypto works.

"There is confusion on who is in charge but that is because there is no regulatory framework. The same confusion we had with Bank of Uganda and Mobile money. For a longtime we grappled with the question of who is the regulator; is it the Bank of Uganda or Uganda Communications Commission? That question was only resolved when the National Payments System was enacted in 2020."

At face value, Dunamiscoins is a basic crypto-Ponzi scheme which should have easily been detected and stopped long before it did massive damage to its investors. Studying the scheme's entire structure, however, shows that the scammers took time to understand and leverage a broken system that offered them one of the easiest avenues into the country's financial and legal systems.

For example, Dunamiscoins set itself as a microfinance entity and that is why it was registered by UMRA. Dunamiscoins exploited the terms of its license which forbid it from taking deposits from customers and instead set up a structure in which investors were shareholders in the scam. The scammers also understood, according to a source with knowledge of the sector that UMRA doesn't do routine checks on its licensees to check if they are complying with the requirements of their respective license. The authority only checks for compliance when a particular entity approaches them for renewal of their license. The schemers built their scam to last for less than a year to avoid that route.

The position of authorities and regulators such as the Bank of Uganda and the Ministry of Finance remains that there is absence of a legal and regulatory framework to deal with crypto related issues including crypto-Ponzi schemes in the country. The message to the public is don't engage and if you do, you are on your own. Yet the actions of the regulators, their political supervisors and the commercial banks tell a different story.

Take, for example, a Bank of Uganda February 14, 2017 press release circulated in the media which warns the general public about operations of a number of crypto schemes, specifically "One Coin Digital Money" in Uganda.

"Bank of Uganda warns the general public that whoever wishes to invest their hard earned savings in Cryptocurrency forms such as One-coin, Bitcoin, Ripple, Peercoin, Namecoin, Dogecoin, Litecoin, Bytecoin, Primecoin, Blackcoin or any other forms of Digital Currency is taking a risk in the financial space where there is neither investor protection nor regulatory purview. The public is hereby warned that whoever deals with "ONE COIN DIGITAL MONEY" does so at his or her own risk," the statement reads in part.

OneCoin did not have market penetration on the scale of Dunamiscoins Resources Ltd but a number of people in Uganda lost money in the scheme. The scheme's founder, Ruja Ignatova, has to-date eluded international arrest warrants to answer for charges in what is dubbed as "one of the biggest scams in history." Prosecutors in the United States claim the scheme brought in

approximately $4 billion worldwide, a sum which is more than a quarter of Uganda's $12.3 billion 2020 national budget. The beneficial owners of Dunamiscoins Kingsley Egbe and Johnson Frank(Nigerians), Isaac Akwete, a Ghanaian and a one Dr Mike(nationality unknown) and Ms. Awon adopted a similar strategy as Ignatova and their whereabouts remain unknown.

A year later, flanked by colleague governors from the East African Community (EAC), a body that unites countries in the region, Bank of Uganda Governor Emmanuel Tumusiime-Mutebile, in February 2018, appears to have a change of heart from the tough stance the institutions he leads had taken on cryptocurrencies, leaving consumers in the open.

"The decentralised nature and multi-country reach of e-currency make it hard to regulate," he said. "In the past, he added, "some central banks either banned or discouraged the adoption of these currencies. However, this approach may no longer be effective given that usage of e-currencies is gaining momentum in some countries".

The statement of Mr. Tumusiime-Mutebile, appears to have no impact on the stance of the organisation that he leads but adds on the mixed messaging and confusion of the public. In June 2019, six months before both the Dunamiscoins Resources Ltd scheme collapsed, Dr. Louis Kasekende, the immediate former deputy Governor of Bank of Uganda, reiterated that there were no regulations on the use of cryptocurrency and anyone involved in using or trading in it was doing so at own risk.

At the time Dr. Kasekende made the remarks in Masaka, Dunamiscoins was in advanced stages of setting up operations in the city west of Uganda's capital Kampala, according to former workers of the company.

The decision would take a while, but Dunamiscoins eventually started operating in the area in November, weeks prior to its collapse, and was welcomed with more than 1,000 people expressing interest to join the company. Many invested while more than 50 people in the area were offered jobs, majority as marketing executives who recruited their friends, relatives and other community members. In a matter of days, the promise of a financial boom ahead of the Christmas festive season turned into a nightmare.

Bank of Uganda is not the only state agency caught up in the cryptocurrencies confusion. A statement by the Minister of Finance, Matia Kasaija, two months before the Dunamiscoins scheme collapsed is more explicit on the government position. He writes on October 1, 2019

that the " government of Uganda does not recognise any crypto-currency as legal tender in Uganda and that the same has not licensed any organisation in Uganda to sell crypto-currencies or to facilitate the trade in crypto-currencies and so these organisations 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 [the] organisation facilitating the use, holding or trading of crypto-currencies fail for whatever reason to deliver the services or value they have promised," Mr Kasaija warned.

Apart from being registered and cleared for operation by two Uganda government authorities, the operations of Dunamiscoins were facilitated by commercial banks under the supervision of Bank of Uganda and in close coordination with the Financial Intelligence Authority. They also operated in communities where the state is present under the purview of the Uganda Police and other local intelligence networks such as the Internal Security Organisation (IS0).

Andrew Kaggwa, the Chief Executive Officer for Global Cryptocurrencies Limited, another crypto-Ponzi scheme which collapsed two days before Dunamiscoins in November 2019, for example, was under the radar of ISO according to several sources at the intelligence gathering outfit and the Police given his past involvement in Ponzi and pyramid schemes that robbed Ugandans of billions. A fugitive, he had fled to neighbouring Rwanda where he started a bakery after one of his schemes collapsed yet he later, quietly, crossed back into the country and resumed his old trade. ISO, Uganda's domestic spy agency only moved to arrest him after his latest scheme collapsed. Many of the Global Cryptocurrencies Limited victims were Uganda military personnel including senior officers.

A year earlier, in November 2018, the Minister of State for Finance (Planning) David Bahati had told Parliament that the government had finalised a law that would regulate crypto assets to prevent criminals from exploiting digital currencies to scam citizens. At the time thousands in Uganda had already lost billions of shillings to Ponzi schemes, including the D9 Club scheme which operated in Uganda, Rwanda and Kenya and promised to pay members in bitcoin.

Unlike in Dunamiscoins Resources Ltd case, Bank of Uganda and other regulatory agencies moved fast on the scheme, freezing much of the money investors had put in the scheme. After

a successful court battle, three commercial banks in the country were compelled to hand over more than Shs7.5bn or $2m to a receiver appointed by the victims.

Mr Bahati's pronouncement was prompted by legislators led by Mathias Mpuuga who tasked the executive to go beyond caution and put in place measures to protect the public.

"If there is no law but you are aware there are agencies operating in the country, who must answer should a problem arise? Can the government at least tell the country [who] the cryptocurrency dealers operating [are]," Mr Mpuuga the representative of Masaka Municipality, the area whose residents would, a year later, be scammed by Dunamiscoins challenged government.

The National Payments Systems Act, 2020, Mr Bahati's magic bullet to crypto-Ponzi schemes in the country only became law in July 2020.

Another legislator Odonga Otto representing Aruu County also raised alarm about the inaction of the regulatory authorities in the country during the same proceeding of the House. "I am currently privy to a case in court of one of the pyramid schemes called D9 that has defrauded many Ugandans, including some MPs, yet there is no legal regime in which people can claim their money," Mr Otto said. The cardinal role of MPs in Uganda is to make laws and under Uganda's constitution, an MP can introduce a Private Members Bill to address a legal lacuna in the event the Executive drags its feet.

In interviews, victims not only appeal to President Museveni to take action and help them recover their money but he is central when it comes to blame for giving cover and investor confidence for the Dunamiscoins resources and other crypto-Ponzi scams.

While the scams guaranteed investors astronomical profits, many people in the country were reluctant to join largely due to the limited knowledge they had of cryptocurrencies and the fear to lose their money. It was President Museveni's launch of the Africa Blockchain Conference in 2018 and the subsequent remarks about the technology that tipped the odds in favour of the scammers. By the time Microfinance Minister, Haruna Kasolo launched Dunamiscoins, according to a journalist cum investor and victim who attended the event at a hotel in Kampala, the potential investors were prepped and ready for the windfall.

While President Museveni and early proponents of cryptocurrencies in the country were in full throttle giving the sector the much needed public relations, the scammers were exploiting the interest created within the population.

In May 2018, President Museveni met with Chinese-Canadian billionaire Zhao Changpeng who was in the country to deliver a keynote address at the Africa Blockchain Conference at the invitation of the Blockchain Association of Uganda. Mr Changpeng is the founder of Binance, the world's largest crypto-currency exchange. In the meeting according to a statement released by the State House, Mr Changpeng told President Museveni that he wants to set up Africa's largest crypto currency exchange in Uganda to lead to the inflow of capital into the country's economy. On his part, President Museveni welcomed the initiative and pledged Uganda's commitment to becoming a global Blockchain destination.

At the conference, President Museveni said Africa is ready for the digital age, insisting that Blockchain technology removes opaqueness in business and replaces it with total transparency. He clashed with Governor Tumusiime-Mutebile who he accused of being "dogmatic" and unwilling to adapt to new technology.

Governor Mutebile had, earlier, told the conference that blockchain technology lacks the necessary prerequisites to work as a currency and that people who sell cryptocurrencies risk being burned when the bubble eventually bursts.

"Cryptocurrencies do not have the privileges of legal tender and are not backed by the central bank, which ensures the supply of the currency is always adequate with the demand. Furthermore, there are no external mechanisms for backing cryptocurrencies to ensure that they have a stable value. Consequently, cryptocurrencies are subject to extreme price volatility which renders them ineffective as a store value or unit of account," Mr Mutebile said.

President Museveni was not amused: "What we're talking about here is to look at new technology as enabling things to move faster and new systems that go with it," he said. He added: "Of course, this is not new and I would encourage the governor to be more inquisitive, not to be dogmatic. I congratulate him for reminding me about my S6 economics of 1966 - the role of money as a unit of account. To tell the value as a medium of exchange and as a store of value. As he knows, money itself changed up to 1930. Initially money was only gold and silver."

Later, in April 2019, President Museveni launched the National Taskforce on the Fourth Industrial Revolution in Uganda. The Block Chain Association of Uganda many of whose members were named on the taskforce equated the move to Neil Armstrong historic moment of setting foot at the moon more than half a century ago.

Kwame Rugunda is the son of Uganda's Prime Minister and Leader of Government Business, Dr Ruhakana Rugunda, and one of the leading voices in promoting Blockchain technology in Uganda. He is the chairperson of the Blockchain Association Uganda. The Harvard educated businessman is also the founder and CEO of CryptoSavannah.

CryptoSavannah is profiled on its website as being at "at the forefront of the blockchain and innovation ecosystem in Africa". Since 2017, the company founders say they have been developing block chain solutions, advising governments and the private sector, and attracting blockchain and crypto companies from around the world to invest in Africa.

Following the collapse of Dunamiscoins and others, Kwame took the flak from legislators and public who accused him of using his father's clout in government to defraud Ugandans. The senior Rugunda was compelled to come out and defend his son. In a statement to Parliament, on February 6, 2020 Dr Rugunda said: "Whereas it is true that my son Kwame is involved in promotion of some of the new technologies within the fourth industrial revolution, such as block chain technology, it is false that his business is associated in any way with Ponzi schemes."

Ponzi schemes would subsist, whether or not the platform leveraged is blockchain technology or another. So, the two need not be conflated according to Dr Rugunda.

"Crypto currencies and Ponzi schemes are two different issues, but the ongoing debate doesn't distinguish them, presenting them as related, the mix up is as a result of Ponzi schemes, referring to themselves as cryptocurrencies, in an attempt to lure people to defraud them."

Minister Bahati also defended Kwame, telling legislators that he was not involved in any crypto-related crime. There is no evidence to suggest any wrongdoing by CryptoSavannah or Kwame, but his leadership of the Blockchain association in Uganda, and being the son of the country's premier, raises possible conflict of interest.

It is these developments and the constant messages of friends making "easy money" that Daisy Namukwaya, a victim, says prompted her to return home from Saudi Arabia to grow the Shs2m or $541 savings she had accumulated from her work as a domestic servant by investing in Dunamiscoins.

"… [I] invest[ed] Shs2m. They told me I would earn 40% profits in 21 days with an offer of 50% increase for the month of December 2019. But the company was shut just a week later. I lost all my deposits and the profits," Ms Namukwaya said.

President Museveni's spokesperson, Don Wanyama, did not respond to my request for an interview or questions.

Those who promote or facilitate the Blockchain technology and cryptocurrencies, in particular, are quick to absolve themselves of any responsibility. Days after it was revealed that a number of crypto-Ponzi schemes had robbed Ugandans of billions in shillings, Patrick Mweheire, the then Stanbic Bank Uganda chief executive, told industry executives at Sheraton Kampala Hotel that Ugandans are better off investing their money in cows than plunging into the unknown world of cryptocurrencies. At the time Mr Mweheire was also the chairman of the Uganda Bankers' Association (UBA).

In the case of Dunamiscoins Resources Ltd, the institution (Stanbic Bank Uganda) and the industry (UBA) which Mr Mweheire led were the conduits of the billions that Ugandans had lost. Between November and December 3, 2020 when the scheme collapsed, Mr Mweheire's bank, Stanbic Bank Uganda, held more than Shs23bn ($6.2m) on behalf of the scam according to former employees of Dunamiscoins which quickly disappeared. In total, three members of UBA, Stanbic Bank, Centenary Bank, and GTrust Bank held a combined total of at least Shs49.5bn ($13.3m) according to various sources who include former accountants and cashiers of Dunamiscoins.

A former public prosecutor Tom Walugembe, who in 2016 successfully prosecuted and secured Uganda's first money-laundering conviction in the case of Uganda v Serwamba David Musoke and Others, says authorities in Uganda have so much at their disposal to deal with the scams.

He cites a number of legislations which authorities can rely on to go after crypto-Ponzi schemes including the recently enacted National Payment Systems Act 2020, the Computer Misuse Act,

2011, the Electronic Transactions Act, 2011, the Anti- Corruption Act, 2009, the Anti-Money Laundering Act 2013 and the Penal Code Act (1950 amended in 2007).

"Like most of the problems in Uganda, the law is not necessarily the problem. I would dare say that we have sufficient laws to deal with crypto-Ponzi scams in Uganda. The above laws provide for a multiplicity of offences under which those behind crypto Ponzi schemes could be prosecuted," he said in an interview.

Mr Walugembe has since moved on from his job as a prosecutor and is now based in Switzerland where he works as an Asset Recovery Specialist with the Basel Institute on Governance, an independent, international non-profit organisation dedicated to preventing and combating corruption and other financial crimes and to strengthening governance around the world. He says Uganda needs to tie the nuts and bolts on regulation.

"In terms of regulation, that is where the challenge lies. Central banks world over are very reluctant to recognise crypto currencies as they are a threat to fiat currencies in the long term. The common approach of central banks such as Bank of Uganda is generally to shun crypto currencies altogether which leads them to basically operate from 'underground' leaving them susceptible to criminal activity," he says.

"A better approach," he adds "would be to have them regulated by setting standards and thus holding those behind them accountable. The only challenge is that some crypto currencies like Bitcoin are configured in a way that they are decentralised [they don't have any central leadership and hence it may not be easy to identify who to hold accountable]."

The archipelago nation of Malta, for example, has developed a strategy and regulatory framework for Distributed Ledger Technologies (DLT) such as cryptocurrency businesses (including exchanges) and virtual assets. The Maltese parliament has enacted three new laws including Malta Digital Innovation Authority Bill, The Technology Arrangements and Services Bill and the Virtual Financial Assets Bill. These according to experts including consulting firm PwC provide "trust, transparency, and security".

It is a view shared by Brian Kalule, a partner at global law firm Bowmans based at their Kampala office.

"The criminal legal framework would deal with them [crypto scammers]. There are many offences under the Penal Code which may apply to such schemes; for instance obtaining money by false pretences, conspiracy to defraud and outright fraud. However, this would require a clear understanding of how these schemes work before charges may be pressed. Unfortunately, the police are usually not well equipped to investigate such complex financial fraud," he says.

Mr Kalule is the Secretary of the legal committee of the Uganda Bankers Association and has published papers about Bitcoin and money laundering. He urges victims of fraudulent schemes to seek legal redress through civil suits.

Lawyer Walugembe attributes the reluctance to the understanding authorities in Uganda attach to cryptocurrencies. He insists the regulators' actions are motivated by their general approach of frowning upon cryptocurrencies as a threat to their fiat currency.

"But the fact is that not all cryptocurrencies are Ponzi schemes. Some of them like Bitcoin are reasonably safe. Part of the bad image of cryptocurrencies has also been caused by the fact that they are normally the currency of choice for organized criminals," he says.

Citing as an example the Silk Road criminal scheme in which drugs were being sold online in the United States and payment being made through bitcoin, Mr Walugembe argues that regulators in Uganda must accept that cryptocurrencies are here to stay and are probably the currency of the future.

"If people chose to engage, they did so at their own risk, with their eyes wide open and in such circumstances their only recourse should be to the courts of law. And by the way, the fact that it is not a regulated activity does not make it illegal. It just means that there is no authority to which the players are answerable and so consumers have to look after themselves," Mr Kalule says.

I formally reached out to senior officials of Bank of Uganda including the Director of Communications and the Executive Director for research who is also the Bank's former acting Deputy Governor. After a week of no response despite constant reminders, I filed an online request to the bank under Uganda's Access to Information law.

On October 13, I received this email response from the "Ask Your Government Uganda" team, a portal set up by government and civil society agencies as part of the implementation of the

Access to Information law. "[The] Bank of Uganda (BoU) has delayed. They have not replied to your ATI request for Crypto-Ponzi schemes in Uganda promptly, as normally required by law," the email reads in part. I was sent a link to remind them about my request which I did.

Commercial banks in Uganda have in place very stringent rules and guidelines on withdrawing large sums of money and in many cases accounts are temporarily frozen until one can prove the source of the said income and its intended use. Last year, for example, Equity Bank Uganda blocked access to money paid to local contractors to transport UN weapons from neighbouring Democratic Republic of Congo to Tanzania's port of Dar es-Salaam until the source could be verified.

Crypto-Ponzi scammers, however, rely on established banks to create a sense of legitimacy around their operations by transacting through these banks. In all the crypto-Ponzi cases, the scammers used established commercial banks to keep and in some cases channel their loot out of the country.

So, at what point were the scams detected. Through sources at the commercial banks, FIA and former employees of Dunamiscoins, I was able to glean a picture of what might have transpired in the days leading to the collapse of Dunamiscoins.

Late November 2019, shortly after the Global Cryptocurrencies Ltd scheme collapsed, Dunamiscoins started missing the deadlines to pay the customers. Subsequently, some of the investors inquired from friends working at the Centenary Bank, which held the largest chunk of the investors' funds, about what might be amiss. It is at this point, 11 months after the scam started, that the bank filed Suspicious Transaction Reports (STRs) with FIA.

"Yes, suspicious transaction reports were raised, but things had already gone wrong. We don't blame the banks because it is typical of Ponzi schemes, they are hard to detect," Mr Asubo says.

Less than 30 minutes after the report was filed, according to internal correspondence, FIA wrote back to the bank to freeze the accounts in Centenary Bank. FIA also wrote to the other banks to check if the scammers had accounts elsewhere. It is at this point that FIA discovered that the scammers had accounts in Guaranty Trust Bank (Uganda) and Stanbic Bank Uganda. Rumours were already circulating in the banking sector of the imminent collapse of the Dunamiscoins "business". When Centenary filed an STR, Stanbic also filed one and FIA wrote

to them to freeze the accounts. Guarantee Trust Bank did not file an STR, but the bank responded to a directive from FIA to freeze the accounts that Dunamiscoins held there after responding to an inquiry from FIA on whether they had accounts for Dunamiscoins. The entire process to end the operations of Dunamiscoins lasted a day, but the Nigerians and a Ghanaian who masterminded the heist, and their co-accused Ugandan director, Susan Awon, had vanished a week earlier.

Dunamiscoins scammers, according to different sources, had a spy network that provided them information to circumvent government dragnets, but this could not be independently verified.

Suspects picked in connection with the scheme claimed they knew nothing about the alleged scam or whereabouts of the missing business owners, and told police detectives that the money was in the bank and the sudden freezing of the company's bank accounts triggered the pay-out crisis.

"Following the collapse of these two companies, Dunamiscoins and Global Cryptocurrencies, we now wrote a circular to the banks giving them a stern warning that banks have an obligation to identify any entity that is operating a Ponzi scheme or cryptocurrency and let us know immediately," Mr Asubo says.

Commercial banks were directed to put in place mechanisms to ensure that if these companies go bust, the investors or customers in the business are protected.

"Many banks told us it is difficult to put in place such mechanisms so the only solution is to close these accounts and many of the accounts have been closed. Investors in the other existing companies have got their money," Mr Asubo adds.

In an interview, a former accountant for the Dunamiscoins Resources Ltd told this journalist that they collected more than Shs1bn ($269,872) on a daily basis starting late April, 2019 when business picked up across the different branches. They paid at least half to the different clients whose payments were due on a particular day.

The former accountant who remains in hiding, having picked money from family and friends to help them invest and also fears being arrested by the police, queries the facts about commercial banks as presented by the police.

Two weeks before the scam collapsed, the accountant said, Centenary Bank had more than Shs26bn ($7m), Stanbic Bank 23bn ($6.2) while GTBank had Shs500 million ($135,073). This was corroborated by another former accountant and cashier with the scam.

An official Uganda Police report, however, indicates a far much lower figure. The Uganda Police report is based on the complaints filed by the victims with the force, which means the unaccounted for monies may have accrued from clients who never filed complaints.

In the April 2020 report, the Police say Dunamiscoins scammers walked away with Shs20bn from at least 2500 people. After the directors allegedly disappeared with the depositor's money, the Police say they recovered Shs47, 000,000 ($12,684) from Dunamiscoins Resources Ltd branches while UGX. 709,000,000 ($191,339) was frozen on the respective accounts by the Financial Intelligence Authority, a government agency set up to combat cases of fraud, money laundering and terrorism financing. The accountant, who as well was an investor and lost personal money, says the questioned police's conflicting figures on the money they recovered from the company.

I contacted the Uganda Police authorities on September 22. They are yet to respond, if at all they will, six months later and despite constant reminders.

From the Ponzi scams they have investigated in the past two decades, the Uganda Police estimates that at least Shs100bn or $27.1m has been stolen from Ugandans by scammers. The Police figure could be conservative given that it is based on those who report to the law enforcement agency and provide evidence of being duped. A number of victims I interviewed say they see no point in reporting to the police and waste more resources because there is no indication that those who have already filed complaints will ever get justice. In other cases, we were informed that highly placed investors including those working in government or major public corporations, suffer quietly in order to protect their public image.

On September 15, I wrote to the commercial banks that operated accounts for Dunamiscoins, inquiring about the specific transactions relating to the Dunamiscoins scheme. A day prior, on September 14, I had reached out to Ms Anne Juuko, the Stanbic Bank Chief Executive Officer. In a message on the following day, September 15, she said that she had designated an official to respond to my questions. She added: "But for confidentiality purposes, I know we will be limited in the amount of info [information] we can share," she said. Cathy Adengo, the Head

of Corporate Communications at Stanbic Bank Uganda did not respond to my questions despite promises to do so.

Allen A. Ayebare, the Chief Manager Corporate Affairs and Communication for Centenary Bank Uganda promised to respond to my questions but lawyered up on September 28.

“Dear Stephen, the case is still under investigation and so cannot be commented on for now,” she said.

The attitude adopted by the commercial banks to my request can be explained by a number of developments during the course of investigations for this story.

In the course of this investigation, the FinCEN Files Scandal broke. The scandal exposed by US based BuzzFeed and the International Consortium of Investigative Journalists (ICIJ) involved more than 2,500 files from the US Financial Crimes Investigation Network sent to authorities in the US between 2000 and 2017, raising concerns about suspicious activity in clients’ accounts.

An employee of one of the commercial banks, who was a liaison contact, said the supervisor hesitated to respond to inquiries because they were unsure of the outcome of this investigation in light of the latest developments in the banking industry.

Apart from the FinCEN files which was a global scandal, banks in Uganda were also facing an onslaught about their alleged predatory lending practices, accusations by customers of other crimes including using dubious means to steal property mortgaged to them by different customers.

On September 9, President Museveni, in response to an appeal by a widow, directed Housing Finance Bank not to sell, or reverse the sale of, her house mortgaged for a loan. The widow simultaneously petitioned the court, challenging the disposal of her property, the Mayflower Apartments, by Housing Finance Bank at $2.4m (about sh8.8b) to a city businessman. According to court documents, the family argues that the property is valued at $8m (about sh29.3b). A subsequent independent valuation put the value at over $9m (about sh33b).

Another incident involves a local businessman who on August 10 sued Diamond Trust Bank in the Commercial Division of the High Court, accusing the commercial bank of facilitating

fraud and money laundering in a Shs43.8bn loan advanced to him. Court, on October 7 ruled in favour of the businessman plunging the banking sector into more chaos.

I put a related question to Mr Walugembe about whether Dunamiscoins Resources Ltd could move such large sums of money out of the banking system without causing any alarm among the regulators and the management of the commercial banks.

“Sadly you and I know that corruption has eaten up the national fabric of our country. It is not difficult to imagine that the culprits use corruption to beat the system. For instance, it is possible that bribes are paid to bankers not to raise Suspicious Transaction Reports (STRs) concerning these schemes,” he said.

“One can also not rule out that even where the STRs are raised, elements within the FIA could be co-opted through bribery so as not to take the necessary action. The culprits could also be beating the system by regularly withdrawing the illicit monies in small and non-reportable amounts; although if the system was robust enough, it would be able to do this up,” he added.

Uganda is a cash economy, and transactions requiring payments in large amounts occur outside the financial system. South Africa’s Financial Intelligence Centre (FIC), for example, has in place **“**cash threshold reporting” requirements which provides the regulators with a mechanism to proactively monitor and report on cash transactions which may be linked to money laundering, terrorist financing activities and other illegal dealings so that potential proceeds of crime are timeously identified and investigated.

Financial institutions and other such businesses in Uganda do not have such a requirement currently. “The Banks only need to understand the source of the money. They do not go ahead to scrutinise the underlying details. That is not their role. The crypto operators were running a business and presumably would say the money source was the business,” Mr Kalule says.

“The banks,” he adds, “had no duty to dig deeper to find out if the business operates ethically or illegally. That would be asking too much of them. In circumstances where persons had been warned not to engage in crypto trade, one cannot expect the banks to protect them.”

Mr Kalule says that while banks have obligations to combat money laundering and financing of terrorism by, for instance, reporting suspicious transactions, they can only do so much.

“This does not turn them into the financial police. Indeed, the banks are in the business of making money. The more money customers have on their accounts, the better for the banks. Their only interest is to understand the source of the money,” he says.

In the course of the investigation, I discovered that Dunamiscoins Resources Ltd had an insurance policy with Jubilee Insurance, one of the leading insurance companies in the country. Potential clients who raised some questions about the authenticity of the scheme were asked to check with the insurance company and Uganda Microfinance Regulatory Authority. A victim who lost more than Shs60m he had saved with his wife said they did the background check at his wife’s insistence and the scheme was cleared by the two Uganda government entities.

I sent Deepak Pandey, Jubilee Insurance’s Chief Executive Officer in Uganda a message. He didn't respond to my request for an interview. Instead he sent me an unrelated image via WhatsApp about ‘Bar Maths’.

“80 bottles of beer minus your age plus 40 bottles of Whiskey equals to the year you were born. Cheers,” it read. I reminded him about my request, but received no reply.

On September 28, I sent him another reminder. He responded: “Hi, I am a bit busy this week,” he wrote. I requested when he could be available or which officer in his organisation he could designate to respond to my requests. He has yet to respond.

In the course of the investigation, I obtained documents indicating that some of “powerful” victims have instead lodged civil proceedings in court against Dunamiscoins and Global Cryptocurrencies. Some of these include Greenlinks International Ltd which has petitioned the court seeking a declaration for breach of contract worth Shs200m plus general damages, interests and costs. Another suit against Dunamiscoins in the same court with similar pecuniary value was filed by Geoffrey Sebuguzi. Other individuals and companies are suing Global Crypto Currencies including Wakanda Safaris Ltd, a tour company, and Ms Costa Nassiwa, a business woman. At the time of writing, all the cases were scheduled for mediation at the Commercial Division of the High Court in Kampala. The planned mediation, however, failed because the defendants neither filed a defence nor had representatives at the mediation hearings.

The victims' attorney, Mr Philp Kasule, declined to respond to my inquiries through WhatsApp and deleted his profile picture after reading my first message. All his clients did not respond to our request for an interview.

On September 17, I contacted a lawyer for another set of victims. Mr Arthur Mpeirwe agreed to an interview on the same day and asked me to send a "questionnaire or at least the hypothesis you are investigating". I did and in response he said "I will consider giving my opinion within the confines of the sub-judice rule since the matter is in court". He declined further comments and ignored subsequent reminders.

In August, about 46 investors who lost money to Dunamiscoins filed a case against Dunamiscoins and FIA. In this particular case, the investors want the court to order FIA to unfreeze the money held on the Dunamiscoins accounts.

Mr Asubo, the FIA executive director, says they will await court decisions to inform their next course of action. In the interim, he says that government must make a decision "…on whether to accept cryptocurrencies or ban them."

"The problem is that the decision is taking long to be made. The crooks are taking advantage of the lack of a regulatory framework to cheat people," he said.

Overview of crypto-Ponzi schemes and how to spot them

Overview of crypto Ponzi schemes and how to spot them

Alert

Promises astronomical returns in a short time
You have to recruit more people
Relentless influencers and network marketing
Unknown business ventures
Exploit new technology and trends
Misleading and incomprehensible details
Ghost owners
Relies on ignorance and greed of potential victims

The scams

Global Cryptocurrencies Ltd
This crypto-Ponzi scheme reportedly stole UGX 10.6BN from at least 425 people according to police reports and court documents.



Dunamiscoins Resources Ltd

At least Shs49.5bn ($13.3m) held by 3 Ugandan banks when Dunamiscoins vanished
Centenary Bank Shs26bn ($7m)
Stanbic Bank 23bn ($6.2)
GTBank had Shs500 million ($135,073).
The Police say Dunamiscoins scammers walked away with Shs20bn from at least 2500 people.



Global trends

In 2019, criminal activity represented 2.1% of all cryptocurrency transaction volume, or roughly $2.14 billion worth of transfers.
The PlusToken Ponzi scheme based in China brought in at least $2 Bn in 2019
$5.2 to $16 Bn lost to the OneCoin scheme in which some Ugandans were victims
South Africa based Mirror Trading International (MTI) was the world's biggest crypto scam of 2020 roping in US$588-million

Numbers

$11.2m
Confirmed amount of money Ugandans lost to criminals cybercrimes in 2019

$27.1m
Amount of money, Uganda Police estimates that at least has been stolen from Ugandans by scammers in the past 2 decades

$4.3 bn
Amount of money Cryptocurrency scammers raked in globally in 2019.

Designed by: STEPHEN KAFEERO
Student's number: 2413461

Reflective Essay

Conducting a journalistic or any type of investigation is hard work. It requires diligence from framing the investigation to post-publishing. It involves unearthing information that many especially powerful individuals and groups want to remain hidden. For example, while leak journalism is definitely not investigative reporting, a leak can be the start of an investigation that brings out more based on a variety of sources. It is sometimes dangerous but rewarding and fulfilling job (Ongowo, 2011).

Whilst I had prior experience conducting investigations as a journalist, my experience conducting an investigation for my for my master's degree was a different ball game. A daunting but enjoyable experience. I started this investigation at the height of the Covid-19 pandemic in South Africa. I was, however, hopeful that the situation would get better and we would resume our "normal lives" including travelling easily and interacting with sources physically. More than a year later, little has changed. I learned to quickly to adapt and come up with new solutions and ideas to execute my project.

In cases where a solution to generate similar results anticipated in the proposal was not possible, I adjusted accordingly by devising mechanisms that would give me a better or closer outcome. For example, I had envisaged a video for the project but travel restrictions, threat of exposure to Covid-19 implied resorting to doing graphics to carry the same message. Using tutorials on YouTube and consultations with experts in the field of computer graphics and design, I taught myself basic design skills that may prove essential in the near future. In all, I was guided by journalistic ethics and incases of a grey area, I consulted my supervisor whose guidance was invaluable.

One of the lessons that I picked from this whole exercise was to reach out to anyone involved or I thought might have something to say or share on the subject under investigation. Most importantly, I allowed them to speak. For example, I let one of the interviewees speak for more than two hours. The first two hours have almost nothing useful but towards the end, he was in his comfort zone and was able to confirm certain things I had discarded as rumours.

I made notes and recordings of everything relating to the project that I did on a particular day and organised them in a way that made sense to me. This was an important lesson almost hammered into my head through the different classes we had with Dr Mark Lee Hunter, Prof Anton Harber and journalists Pauli Van Wyk and Ron Nixon. This helped me in terms of confidence that I was making progress, allowed me to make follow ups and when it came to

writing, to structure my story given that I could locate all my content from the different sources.

The lockdown was tough but it provided me an opportunity to concentrate on the bigger picture. Thanks to the generous scholarship from the Open Society Foundation South Africa, I had decent and safe accommodation with largely all the things that I needed to work on my projects. My priorities were also not at cross purposes given that my basic needs were taken care of and I didn't have to divide my attention between surviving and doing the only work that mattered.

My investigation was designed to be executed mostly in Uganda and as I discuss later, the inability to fly home implied had its advantages and disadvantages. I couldn't, for example, do face to face interviews which deprived the investigation an opportunity to record the emotions of the sources but also push some to speak. Many of the victims are in the informal sector and are not tech savvy which implied that I could not rely on such things as Skype and Zoom to interview them. The upside of this was, it challenged me to think deeply about my work and come up with solutions that would not only prove to be key for the investigation but also offer a template for my future work as an investigative journalist.

Interviews

Interviewees for the investigation were targeted based on their role in the scam. I reached out to the victims for their personal stories including the impact that the scam had on their lives. Public officials and organisations whose action or inaction perpetuated the scam were also targeted and either interviewed or their roles documented. For insights, I also reached out to independent observers with knowledge of the subject. The whereabouts of the key people who initiated the scam remain unknown and therefore could not be reached but former employees and associates were interviewed in an attempt to develop insights into what exactly happened.

Efforts were also made to study and review a number of jurisdictions that have suffered similar challenges like the subject of the investigation as part of efforts to develop knowledge of the subject but also to pick lessons in terms of solutions and challenges.

In some of the interviews, I found that government and commercial bank officials, especially, were evasive in their responses and some simply chose not to respond at all despite being given all the time they required.

The failure to get explanations and insights from some of these officials left me disillusioned and distraught about my investigation. However, I had not only been prepared for this through

prior discussions with my classmates and professors but it was also a clear reminder of the importance of investigative journalism. It exists to poke holes and even open the close doors.

Most of the respondents were in Uganda whilst I was based in South Africa. This presented both an opportunity and challenge. Some off the record sources did not want talk on phone or through common messaging apps like Whatsapp. I had to resort to more secure alternatives such as Signal and Telegram but this also required taking them through the basics of the platforms and convincing them that the same were secure.

To sources I had not interacted with before, it also meant building a relationship of trust which is hard to do through digital platforms. Ideally, I would have suggested a physical meeting at their office or over some drinks but this was not possible. I solved this by convincing the sources that this was an academic pursuit and not a purely journalism project due for publication in the newspaper. “I don’t want to be part of your headlines in the Monitor newspaper, one source told me.” The Monitor newspaper is Uganda’s leading independent daily and a place I worked until I embarked on my studies at the Wits University. My role as an “Investigations and Special Projects” reporter meant that I upset so many quarters. I suspect that those who renegaded on appointments and promises for information read my profile and decided it was not in their best interest to speak to me. While I pushed, I respected the choices of those who wished not to speak or changed their mind. For those who showed willingness to discuss their role in the matter under investigation but opted to pull out or stopped communicating, I detailed the process in investigation piece.

Despite the distance and technology challenges, the victims mostly poor working class individuals were more cooperative. This was a poignant lesson, one I had learned in the series of lectures with my professors but one I hadn’t paid so much attention to in practice. Given my understanding of the cultural nuances of the affected individuals gave me an edge. The fact that I was also in a different country reaching out to victims largely ignored by the local press also boosted my chances of getting feedback. As one source told me during an interview, she was happy “someone was asking the questions”. Still, the source had reservations on the impact of my research in as far as alleviating their predicament was concerned. In the end I realized some of the information sought from government and commercial bank sources could be gleaned from reports and other documents. The refusal to engage also offered me an opportunity to put to test Uganda’s access to information regime. Again, this is something we had explored in our

respective lectures as a key feature, investigative journalists can use to hold public agencies to account per established law

While Uganda passed a law on access to information in 2005, the Access to Information Act which operationalized and gave effect to Article 41 of the 1995 Constitution. It has been widely ignored by both those it intends to help (citizens and journalists) and those who are obliged to obey it (public agencies and officials).While a section of the civil society and international donors have invested heavily to create platforms to ensure the aspirations of the framers of the law are met, the idea is seen as slow and impeding journalism work including frustrating "scoops". Many investigative journalists including myself have not used the mechanisms envisaged in the law to seek for information and so my first attempt during my investigation was an eye opener despite the negative results. The respondents are yet to give feedback although months have passed after the period granted to them under the law.

Generally, the process was a challenging despite the luxury of time the project afforded me. The longest investigation I had conducted prior lasted three months but for this project I had more time but things never go as planned even when one has a lifetime to execute a project. I was, however, prepared to be flexible and resilient. A quick example is when a source promised to leak to me a "government whitepaper" detailing internal investigations by government bodies into various scams and proposed solutions. I was excited because this meant I could flag the same information to key players who were unwilling to speak. The source didn't come through and to-date cites fear for security of their own job and other factors such retribution from named colleagues. I had to re-strategise which implied reaching out to more people to glean a picture of what really happened and the ongoing conversations within government.

References

Akshay, A. K. (2020, June 22). Biggest Ponzi Schemes in the History of Crypto. Retrieved July 31, 2020, from https://eng.ambcrypto.com/biggest-ponzi-schemes-in-the-history-of-crypto/

Al Jazeera. (2018, March 24). Uganda's bitcoin enthusiasts. Retrieved June 30, 2020, from https://www.aljazeera.com/news/2018/03/uganda-bitcoin-enthusiasts-180324100659082.html

Allmark, P., Boote, J., Chambers, E., Clarke, A., Mcdonnell, A., Thompson, A., & Tod, A. M. (2009). Ethical Issues in the Use of In-Depth Interviews: Literature Review and Discussion. *Research Ethics, 5*(2), 48-54. doi:10.1177/174701610900500203

Allmen, U. V., Khera, P., Ogawa, S., & Sahay, R. (2020, July 02). Digital Financial Inclusion in the Times of COVID-19. Retrieved July 29, 2020, from https://blogs.imf.org/2020/07/01/digital-financial-inclusion-in-the-times-of-covid-19/

Among, I., & Munavu, M. M. (2019). 'We want to be heard': The voices of Uganda's young people on youth unemployment. Retrieved July 29, 2020, from https://blogs.worldbank.org/nasikiliza/we-want-to-be-heard-the-voices-of-ugandas-young-people-on-youth-unemployment

Ana. (2019). Flashy cars, parties, cash payouts – all part of Ladysmith 'investment scheme'. Retrieved July 21, 2020, from https://citizen.co.za/news/south-africa/local-news/2142537/flashy-cars-parties-cash-payouts-all-part-of-ladysmith-investment-scheme/

Bagala, A. (2020, September 20). Masters of the con game. Retrieved December 07, 2020, from https://www.monitor.co.ug/uganda/news/national/masters-of-the-con-game-2303940

Bartlett, J. (2019, November 24). Cryptoqueen: How this woman scammed the world, then vanished. Retrieved August 13, 2020, from https://www.bbc.com/news/stories-50435014

BBC. (2019). Uganda Media Landscape Report. Retrieved December 7, 2020, from https://www.communityengagementhub.org/wp-content/uploads/sites/2/2019/09/Uganda-Media-Landscape-report_BBC-Media-Action_February-2019.pdf

Beasley, C., & Walker, L. (2014). Research ethics and journalism in the academy: Identifying and resolving a conflict of culture. *Research Ethics, 10*(3), 129-140. doi:10.1177/1747016114531981

BOU, B. (2011). Financial Consumer Protection. Retrieved December 06, 2020, from https://bou.or.ug/bou/bouwebsite/FinancialInclusion/consumerprotection.html

Darby, M. (1998, December 01). In Ponzi We Trust. Retrieved July 16, 2020, from https://www.smithsonianmag.com/history/in-ponzi-we-trust-64016168/

Dickinson, A. (2019, February 14). Journalism ethics Vs. Research ethics. Retrieved August 10, 2020, from https://andydickinson.net/2018/12/14/journalism-research-and-the-academic/

Feikert-Ahalt, C. (2019, April 01). Malta. Retrieved July 21, 2020, from https://www.loc.gov/law/help/cryptoassets/malta.php

Fensham, P. J. (1985). Science for all: A reflective essay. *Journal of Curriculum Studies, 17*(4), 415-435. doi:10.1080/0022027850170407

FIC. (2019). Financial Intelligence Center: Case Studies and Indicators Collection. Retrieved July 30, 2020, from https://www.fic.gov.za/Documents/CASE%20STUDIES%20&%20INDICATORS%20COLLECTION%20final.pdf

Greeff, M. (2020, May 05). CONDUCTING QUALITATIVE RESEARCH DURING A PERIOD OF ... Retrieved August 13, 2020, from https://rcd.mandela.ac.za/rcd/media/Store/documents/Research%20Ethics/Research%20Ethics%20Committee%20Human/Final-Qualitative-research-during-the-Covid-19-pandemic_Minrie-Greeff.pdf

Hall, J. (2018, May 20). What Is Cryptocurrency? A Simple Guide To Understanding Cryptocurrency And Crypto News. Retrieved August 03, 2020, from https://www.forbes.com/sites/johnhall/2018/05/20/what-is-cryptocurrency-a-simple-guide-to-understanding-cryptocurrency-and-crypto-news/

How to organize and write an investigative journalism story. (2012, July 02). Retrieved December 04, 2020, from https://ijnet.org/en/story/how-organize-and-write-investigative-journalism-story

Hunter, M. L. (2011). *Story-based inquiry: A manual for investigative journalists*. Paris: UNESCO.

Hunter, M. L. (2011). *Story-based inquiry: A manual for investigative journalists*. Paris: UNESCO.

The Independent, T. (2019, September 30). Gov't tells Ugandans to stay away from cryptocurrencies. Retrieved August 10, 2020, from https://www.independent.co.ug/govt-tells-ugandans-to-stay-away-from-cryptocurrencies/

Kaiser, K. (2009). Protecting Respondent Confidentiality in Qualitative Research. *Qualitative Health Research, 19*(11), 1632-1641. doi:10.1177/1049732309350879

Kamusiime, W., & Isah, S. (2020, April 28). IGP launches 2019 Annual Crime Report. Retrieved June 30, 2020, from https://www.upf.go.ug/igp-launches-2019-annual-crime-report/

Kavuma, R. (2016, January 13). Ugandan financial fraud victims: Still fighting for compensation years later. Retrieved July 16, 2020, from

https://www.theguardian.com/global-development-professionals-network/2016/jan/13/ugandan-victims-still-fighting-for-compensation-years-late-cowe

Kazibwe, K. (2019, December 02). How thousands including UPDF general were fleeced of billions in cryptocurrency scam. Retrieved August 13, 2020, from https://nilepost.co.ug/2019/11/28/how-thousands-including-updf-general-were-fleeced-of-billions-in-cryptocurrency-scam/

Kazibwe, K. (2019, December 02). How thousands including UPDF general were fleeced of billions in cryptocurrency scam. Retrieved August 13, 2020, from https://nilepost.co.ug/2019/11/28/how-thousands-including-updf-general-were-fleeced-of-billions-in-cryptocurrency-scam/

Kazibwe, K. (2019, May 15). The 18 pyramid schemes that have fleeced Ugandans of billions. Retrieved July 30, 2020, from https://nilepost.co.ug/2018/12/09/the-18-pyramid-schemes-that-have-fleeced-ugandans-of-billions/

Kimbowa, J. (2018, January 03). Nine ways you can be conned in 2018. Retrieved July 16, 2020, from https://observer.ug/lifestyle/56521-nine-ways-you-can-be-conned-in-2018.html

Kuhn, D. (2019, July 08). Crypto Ponzi Scheme Says It Has 'No Cash to Pay out' to Upset Investors. Retrieved July 21, 2020, from https://www.coindesk.com/crypto-ponzi-scheme-says-it-has-no-cash-to-pay-out-to-upset-investors

Kushaba, A. (2016). COWE Scam Victims Commit Suicide. Retrieved July 16, 2020, from https://ugandaradionetwork.net/story/12-years-later-cowe-victims-yet-to-give-up-

Masereka, A. (2019, April 12). REVEALED: Details Of 4th Industrial Revolution Task-force Launched By Museveni Leak " Business Focus. Retrieved August 10, 2020, from https://businessfocus.co.ug/revealed-details-of-4th-industrial-revolution-task-force-launched-by-museveni-leak/

Masie, D. (2018, February 11). Why it would be in everybody's interests to regulate cryptocurrencies. Retrieved August 26, 2020, from https://theconversation.com/why-it-would-be-in-everybodys-interests-to-regulate-cryptocurrencies-91168

Morris, D. (2017, May 31). The Rise of Cryptocurrency Ponzi Schemes. Retrieved July 30, 2020, from https://www.theatlantic.com/technology/archive/2017/05/cryptocurrency-ponzi-schemes/528624/

Muhangi, K. (2020, April 16). About Bitcoin and regulation by Bank of Uganda. Retrieved August 10, 2020, from https://www.newvision.co.ug/news/1497846/about-bitcoin-regulation-bank-uganda

Nakaweesi, D. (2020, June 30). National Payment Systems law gives industry legitimacy. Retrieved August 10, 2020, from https://www.monitor.co.ug/Business/Prosper/National-Payment-Systems-law-gives-industry-legitimacy/688616-5584962-116dr3c/index.html

Nazakat, S. (Ed.). (2017). Investigative Journalism Manual. Retrieved December 6, 2020, from http://www.investigative-manual.org/wp-content/uploads/2016/09/Investigative-Journalism-Manual.pdf

Odyek, J. (2019, June 28). Bank of Uganda warns public on online cryptocurrency. Retrieved August 10, 2020, from https://www.newvision.co.ug/news/1502661/bank-uganda-warns-public-online-crypto-currency

Ongowo, J. O. (2011). CHAPTER 1 DEFINING investigative reporting what makes it ... Retrieved April, from https://ccnmtl.columbia.edu/projects/caseconsortium/casestudies/23/casestudy/files/sun sentinel/coronel_chapter_10_16.pdf

Opencoprates. (2020). DUNAMISCOINS RESOURCES LTD. Retrieved June 30, 2020, from https://opencorporates.com/companies/ug/80020001481676

Pisani, W. (2018). The Malta Virtual Financial Assets Act. Retrieved July 21, 2020, from https://www.grantthornton.com.mt/industry/fintech-and-innovation/The-Malta-Virtual-Financial-Asset-Act/

Richards, I. (2010). Journalism's Tangled Web: Business, Ethics, and Professional Practice. *Journalism Ethics,* 171-180. doi:10.1093/acprof:oso/9780195370805.003.0011

Rosic, A. (2016, July 13). What is Cryptocurrency: [Everything You Need To Know!]. Retrieved August 03, 2020, from https://blockgeeks.com/guides/what-is-cryptocurrency/

S. (2013, July 1). Investor alert Ponzi schemes using virtual currencies. Retrieved August 31, 2021, from https://www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf

Sadiraj, K., & Schram, A. (2018). Inside information in Ponzi schemes. *Journal of the Economic Science Association, 4*(1), 29-45. doi:10.1007/s40881-018-0047-4

Scott, B. (2016, February). How Can Cryptocurrency and Blockchain Technology Play a ... Retrieved August 26, 2020, from http://www.unrisd.org/80256B3C005BCCF9/%28httpAuxPages%29/196AEF663B617144C1257F550057887C/$file/Brett%20Scott.pdf

Sengers, L., & Hunter, M. L. (2012). The Hidden Scenario: Plotting and Outlining Investigative Stories (Logan Handbooks) eBook: Sengers, Luuk: Amazon.co.uk: Kindle Store. Retrieved August 27, 2020, from https://www.amazon.co.uk/Hidden-Scenario-Outlining-Investigative-Handbooks-ebook/dp/B00900WRB6

Supra, J. (2018, April 5). Cryptocurrencies, blockchain and Ponzi schemes. Retrieved August 31, 2021, from https://www.jdsupra.com/legalnews/cryptocurrencies-blockchain-and-ponzi-81594/

Tajti, T. (2019). (PDF) Pyramid and Ponzi Schemes and the Price of ... Retrieved August 1, 2020, from https://www.researchgate.net/publication/336532894_Pyramid_and_Ponzi_Schemes_a

nd_the_Price_of_Inadequate_Regulatory_Responses_A_Comparative_Account_of_the_Diverging_Regulatory_Responses_of_China_Europe_and_the_United_States_In_5_Texas_Tech_Business_an

Uganda Police. (2020). Uganda 2019 Crime & Safety Report. Retrieved July 09, 2020, from https://www.osac.gov/Content/Report/a1b6c9ff-453a-4818-97c5-15f4aeba3246

Zeija, F. (2018). Consumer Protection in Uganda: The Law in Theory and Practice. *Journal of Consumer Policy, 41*(4), 455-471. doi:10.1007/s10603-018-9382-3