

The nexus between blockchain distributed ledger technology and financial crimes

Newton Chinyamunjiko¹, Forbes Makudza^{2*}, Lucia Mandongwe³

Department of Accounting and Finance, Midlands State University, Gweru, Zimbabwe¹

Department of Business Management, Manicaland State University of Applied Sciences, Mutare, Zimbabwe²

Department of Accounting, Manicaland State University of Applied Sciences, Mutare, Zimbabwe³

newtonchinya@gmail.com¹, forbesmakudza@gmail.com^{2*}, lucia.mandongwe@staff.msuas.ac.zw³



Article History

Received on 8 September 2021

1st Revision on 13 October 2021

2nd Revision on 28 October 2021

Accepted on 9 November 2021

Abstract

Purpose: The study sought to uncover the effect of blockchain digital ledger technology (BCDLT) on financial crimes. The study was driven by the need to promote blockchain technology in a bid to enhance financial sanity through the elimination of financial delinquency.

Research methodology: The study followed a quantitative paradigm using an explanatory research design. The study targeted financial executives, senior staff members at the Zimbabwe stock exchange, bankers, and officials from the financial regulators. Data was collected using a structured questionnaire.

Results: The study found that of the four independent BCDLT antecedents, manual audit costs were insignificant, whereas the other three had strong positive associations with financial crime reduction.

Limitations: The study targeted a specific group of financiers; hence the results may not be universal to other excluded categories

Contribution: The study significantly guides policy formulation and laws in line with the adoption of blockchain technology in the global financial system to guard against the possibility of new forms of financial crimes that could emanate from the use of technology.

Keywords: Blockchain digital ledger technology, Financial crime, Financial performance

How to Cite: Chinyamunjiko, N., Makudza, F., & Mandongwe, L. (2022). The nexus between blockchain distributed ledger technology and financial crimes. *International Journal of Financial, Accounting, and Management*, 4(1), 17-30.

1. Introduction

As a result of the evolution of technology, financial crimes are proliferating and spreading like a veld fire into a more sophisticated mishmash. In this highly globalized and technologically advanced world, blockchain technology is gaining prominence as a tool to curb financial crimes. [Wadey \(2019\)](#) stated that the exact global statistics in relation to financial crimes are hard to determine with accuracy, especially given that many cases thereof are not reported. However, the same author pointed out that figures in outstanding cases are evidence of how big the problem is, for example, in May 2016, a Japanese retail business (7-Eleven stores) lost \$13 million which was stolen from its ATMs. In a USA ATM fraud, US\$45m was fraudulently withdrawn in two separate attacks.

Blockchain ledgers are decentralized and shared computer digital ledgers whose transactions are updated in real-time and are confirmed by all participants on the network without the need for a central counterparty. The blockchain digital ledger system forms time-stamped blocks of transactions that are then linked to previous blocks to form a chain of blocks stored and accessed by all nodes on the network ([Zarpala & Casino, 2020](#)). Blockchain distributed ledger technology has received widespread attention after an efficacious boom of Bitcoin. A number of studies were performed on this technology with some scholars questioning its importance, degree of security, and trustworthiness in financial spheres ([Huang](#)

[& Trangle, 2020](#); [Jung & Lee, 2017](#); [Gottschalk, 2010](#); [SestremOchôa, et al., 2021](#)). Prior studies have shown that there is still debate on whether blockchain distributed ledger technology will aid in reducing financial crime or will give birth to new complex financial crimes.

There has also been an increase in companies reporting losses due to financial crimes globally. Losses reported range from US\$10m to US\$19.9m ([Wadey, 2019](#)). [Polyviou, Velanas, and Soldatos \(2019\)](#) state that in February 2016 alone, \$81m was stolen from Bangladesh Central Bank. Coming to Africa, [Wadey \(2019\)](#) revealed that US\$67bn was lost in Africa due to banking fraud in 2014 alone. An investment climate survey carried out by World Bank showed that over 29% of African business people believe that the major constraint on investment is a crime ([United Nations Office on Drugs and Crime, 2005](#)).

In fact, one group of scholars is of the view that blockchain digital ledger technology is very effective in reducing financial crimes, for example, [Zarpala and Casino \(2020\)](#) concluded that embezzlement of funds by bank employees could be significantly reduced by blockchain through pairing hashes with real-time synchronized information to guarantee a trail of events and preservation of a chain of custody. [Polyviou, Velanas and Soldatos \(2019\)](#) are of the view that crime reduction can be aided by an effective and efficient know your customer (KYC) process enabled by blockchain. More so, [Liu and Xu \(2019\)](#) highlight that the use of blockchain can significantly free auditors from the traditional evidence gathering activities, thus leaving them with enough time for performing financial advisory roles. Still, on that school of thought, [Mantelaers, Zoet and Smith \(2019\)](#) concluded that triple-entry blockchain accounting provides an opportunity for a more efficient and effective audit, thereby curbing financial crimes.

On the contrary, another school of thought believes that blockchain ledger technology would in fact aid or promote the commission of traditional and new complex crimes, for example, [KPMG \(2018\)](#) states that the anonymity of transacting parties associated with cryptocurrency makes it difficult for banks to monitor transactions. In the same line of argument, the [International Federation of Accountants \(2018\)](#), observed that when it comes to permission, there is no legal recourse available to participants. [Gilmore \(2017\)](#) argues that blockchain technology is prone to abuse by criminals paying bribes and other nefarious bonus funds through dark markets that are fueled by cryptocurrencies such as bitcoin. [Gilmore \(2017\)](#) goes on to give the example of the “Silk Road” dark market that was cracked down and closed by the New York Department of Financial Services. The Silk Road example was also mentioned by [Rigsby \(2016\)](#) who explained how its founder, Dread Pirate Roberts, operated it for illicit drug trading.

In support of the foregoing, [Bank International for Reconstruction and Development/ the World Bank, \(2017\)](#) also highlighted challenges such as cybersecurity and operational security that can come with the adoption of the blockchain digital ledger technology. [British Bankers’ Association \(2015\)](#) also pointed out that what makes the enforcement of anti-money laundering regulations and other financial crime regulations very difficult these days is the fact that banks and other enforcement units now need to adapt and have a reliance on systems that are outside their control, for example, blockchain’s Bitcoin, Apple Pay, and PayPal.

That ambiguity associated with the blockchain technology’s distributed ledger prompted the need for this study, so as to analyze and examine how and the extent to which the blockchain technology can reduce financial crimes, if at all, and to explore the possibility of the rise of new complex financial crimes that could result from worldwide adoption of the technology. The main objective of the study, therefore, was to examine the differential effect of blockchain digital ledger technology (BCDLT) antecedents on financial crime management. Furthermore, the study assesses the extent to which blockchain technology can reduce or eradicate existing financial crimes by eliminating third parties in financial transactions. The study significantly guides policy formulation and laws necessary for enactment *pari passu* with the adoption of the blockchain technology in the global financial system to guard against the possibility of new forms of financial crimes that could emanate from using the technology.

2. Literature review

Unpacking Financial Crime

Financial crime had no universally accepted definition until the final part of the 20th century, where its scope was restricted. It is understood as every nonaggressive criminality that usually results in an economic loss ([International Monetary Fund, 2021](#); [Jung & Lee, 2017](#); [Gottschalk, 2010](#)). The UK's [Financial Services and Markets Act 2000](#) Section 6(3) views it as 'any offense involving fraud or dishonesty; misconduct in or misuse of information relating to, a financial market; or handling the proceeds of crime'.

A financial crime is any non-violent crime that causes financial loss ([Wadey, 2019](#)). Consequently, financial crime encompasses a wide range of crimes ranging from insider trading, money laundering, tax evasion, corruption, and even terrorist financing ([Violeta, Vaidean, Borlea, & Florescu, 2021](#)). Generally, financial crime is escalating as measured by an increase in fraud and money laundering data captured by 2018 ([United Nations Office on Drugs and Crime, 2021](#); [INTERPOL, 2021](#)). Financial crime affects individuals and organizations, both on local and international platforms. Studies have indicated that globalization and financial market assimilation motivates financial abuse ([International Monetary Fund, 2021](#)).

The Anatomy of Blockchain Distributed Ledger Technology

The blockchain notion was introduced in 2008 as a public ledger, recording bitcoin currency (Sestrem Ochôa, et al., 2021; [Huang & Trangle, 2020](#)). Blockchain is a technology, which runs a volume of cryptocurrencies, but its objective is not to facilitate financial crime. It possesses numerous applications all over the whole lawful economy and it assures security and confidentiality in the transactions performed ([European Parliament, 2018](#); [International Finance Corporation, 2021](#)). A blockchain is a type of distributed ledger technology, however, it is vital to underscore that not all distributed ledgers can be classified as blockchains. The blockchain works with an encryption technique recognized as cryptography. In a blockchain, there are interrelated data blocks that form a chain. Distributed Ledger Technology is a system of capturing and distributing data through several data stores (Ledgers), with each possessing exactly the same data records. They are collectively maintained and controlled by a distributed network of computer servers, which are called nodes. This digital system requires no intermediary or a centralized trusted third party, as shown in Figure 1.

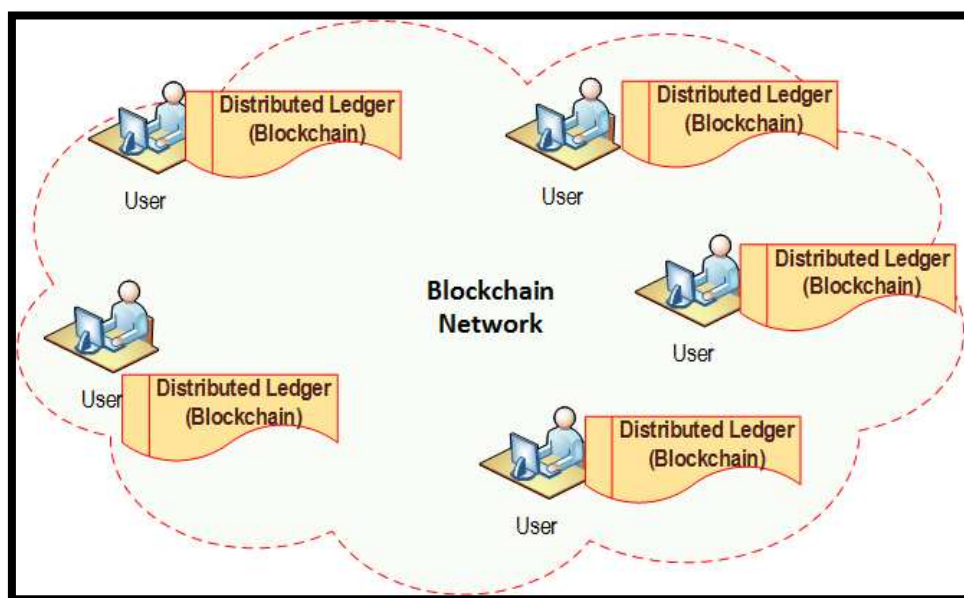


Figure 1. Blockchain distributed ledger technology

Source: Adapted from [Rawat and Doku \(2020\)](#)

There is a belief that the blockchain technology which effectively eliminates the need for third parties such as clearing houses, bourses for shares and futures, and central counterparties, has the capacity to reduce risk and fight financial crimes associated with those third parties such as insider trading, benchmark price tweaking or rigging and fraud (DBS Group research, 2016). Contrary to the foregoing, the [British Bankers' Association \(2015\)](#) believes that with the advent of blockchain ledger technology and associated virtual currencies, comes the increased difficulty in curbing financial crimes.

The development of commerce culminated in the complexity of transactions and the ever-increasing distances between transacting parties called for the need for intermediaries such as banks and securities depositories to process, maintain and track transactions. A clearing house thus has the need to verify the work of the intermediaries at an increased cost of the transaction. The advent of blockchain technology's distributed ledger is primarily aimed at eradicating the cost of transacting (DBS Group research, 2016).

Augmenting the adoption of blockchain technology through policy and law frameworks

[Gilmore \(2017\)](#) observed that since the computer code regulates the behaviour of the users pretty much the same way as a legal code of law, then it stands to reason that it must be accorded the same status as the actual conventional legal code of law. Corollary to the foregoing, if at all the computer code is to be given the status of a code of law and it regulates the conduct of people transacting using blockchain ledger technology, it stands to reason that the traditional lawmakers' (parliamentarians) role of making laws will be usurped by the programmers and or designers of blockchain ledger technology. In fact, the question is, will the code design be inspired by the general populace in line with principles of democracy or it will be as per the whims of the designers? [Gilmore \(2017\)](#) however, was quick to mention that although a computer code can be useful and efficient in regulating the behaviour of people, it is not without its numerous limitations. In fact, [Gilmore \(2017\)](#) noted that the blockchain applications are not really in sync with the existing laws so much so that several efforts were made of late to try to whip the bitcoins (currency of the blockchain ledger technology) in line with existing laws.

Another fallacy of the distributed ledger technology is that says participants in the network would not need a trusted central party to verify data before recording it. Instead, according to [International Bank for Reconstruction and Development/ the World Bank \(2017\)](#), they would use what is called a consensus mechanism – a validation method that is cryptographically programmed and built into the blockchain system to ensure the agreement of all nodes before a block can be added.

To buttress the fact that current regulation and monitoring systems are not enough for blockchain transactions, [KPMG \(2018\)](#) stated that the anonymity of transacting parties associated with cryptocurrency makes it difficult for banks to monitor transactions. In the same line of argument, the [International Federation of Accountants \(2018\)](#), observed that in permission-less blockchain networks there is no legal recourse available to participants. Blockchain technology is prone to abuse by criminals paying bribes and other nefarious bonus funds through dark markets that are fuelled by cryptocurrencies such as bitcoin ([Gilmore 2017](#)). The same author went on to give the example of the “Silk Road” dark market that was cracked down and closed by the New York Department of Financial Services. The Silk Road example was also mentioned by [Rigsby \(2016\)](#) who explained how its founder, Dread Pirate Roberts operated it for illicit drug trading.

Formulation of new laws and amendments to existing ones.

In view of the foregoing, it means that there is a need for formulation of new anti-money laundering laws, for example, taking a cue from the state of West Virginia which amended its money laundering laws to make it a serious crime to be using bitcoins for money laundering purposes. These amendments, however, could still amount to nothing if parties transacting using the blockchain ledger technology remain anonymous to each other ([Gilmore 2017](#)). [Rigsby \(2016\)](#), in support of [Gilmore \(2017\)](#), noted that by virtue of them being financial in nature, the virtual currency and blockchain ledger technology are the most important targets of the counter financing of terrorism and anti-money laundering new laws to be formulated and or amended. [Rigsby \(2016\)](#) cited the demise of the Mt. Gox Bitcoin exchange

market in Japan as a clear indication that unregulated virtual currency exchanges are a great risk to investors, who in this particular case lost millions worth of Bitcoins.

The [International Finance Corporation \(2017\)](#), however, see a ray of light if the peculiar features of blockchain technologies are accommodated in the new regulations to recognize their legal validity in terms of digital identities created by them, Know Your Customer checks done by them, its mechanisms for dispute resolutions as well as its smart contracts.

Financial Crime Reduction Capabilities of Blockchain Technology

The [International Finance Corporation \(2017\)](#) observed that whilst costs of enforcing Anti-Money Laundering regulations and a host of other laws fighting financial crimes are rising sharply, a secure digital identity established by blockchain technology offers a cost-effective way of managing regulatory requirements. The organization further noted that the current duplication of effort by financial institutions in performing Know Your Customer checks can also be done away with because once a thorough verification and validation are done, the document can then be shared on the blockchain network.

In view of the foregoing, [International Finance Corporation \(2017\)](#) believes in the ability of blockchain technology to reduce financial crimes by virtue of it being a cost-effective and decentralized regulatory requirement management system. In fact, the organization ([International Finance Corporation](#)) sees great potential in blockchain technology to support the enforcement of regulations in the future. Know Your Customer syndication by governments and financial institutions in compliance with Anti-Money Laundering regulations is going to be made even easier through the adoption of blockchain technology ([International Finance Corporation 2017](#)).

In that same line of argument, [Microsoft \(2018\)](#) states that blockchain technology can reduce the cost of processing information and reduce the risks of financial crimes as digitalized information about transacting parties will be in digital lockers for all to see. Again, traditionally siloed information will be integrated by the blockchain, and thus no chances of cheating and fraud, especially in insurance claims. [Microsoft \(2018\)](#) also observed that non-conformance to regulatory requirements by financial service providers such as banks does not only attract huge fines for the service providers but also puts customers at risk of being exposed to criminal behaviour. On the other hand, compliance to regulatory requirements (which are necessary to curb crime) is not easy due to several reasons that include the need to do manual and time-consuming audits while at the same time relying on data from traditionally duplicative and siloed data sources.

Corollary to the foregoing, the aggregation of information from previously siloed data sources by blockchain technology will make compliance with regulations automated and unquestionably reliable and quick ([Microsoft, 2018](#)). In fact, [Microsoft \(2018\)](#) believes that systems such as Corda cannot only reduce costs of processing information but can significantly curb the occurrence of multiple versions of truths that are associated with manually verified data, much to the chagrin and annoyance of fraudsters who up to now ride on siloed data. Digital Ledger technology is potentially more resilient to cybercrime due to the decentralized nature of the system. In fact, databases that are centralized are easier to attack because there is a central point that can be targeted for paralysis ([International Bank for Reconstruction and Development/ the World Bank 2017](#)).

Modelling of financial crime reduction

Know Your Customer syndication by governments and financial institutions in compliance with Anti-Money Laundering regulations is going to be made even easier through the adoption of blockchain technology ([International Finance Corporation 2017](#)). [Harvard Law School \(2020\)](#) stated that the costs incurred by banks in vetting new customers who want to open accounts can be drastically reduced or done away with completely through the adoption of blockchain technology. This process of doing due diligence and vetting a new customer is called Know Your Customer (KYC). Once information is stored in the blockchain file by one bank, all the connected banks to the platform would in the future be able

to use the same information without repeating the process of due diligence and vetting. Only amendments or additions to the information stored would in the future be required.

[Polyviou, Velanas, and Soldatos \(2019\)](#) in support of the usefulness of blockchain in KYC argued that the traditional KYC/KYB process is daunting work of creating profiles and documents, specially made so because of the evolving nature of applicable regulations. To them, blockchain would aid a lot in the reduction of KYC costs and work -and greatly aid in reducing financial crimes. In that same line of argument, [Microsoft \(2018\)](#) stated that blockchain technology can reduce the cost of processing information and reduce the risks of financial crimes as digitalized information about transacting parties will be in digital lockers for all to see. Again, traditionally siloed information will be integrated by the blockchain, and thus no chances of cheating and fraud, especially in insurance claims.

[Microsoft \(2018\)](#) also observed that non-conformance to regulatory requirements by financial service providers such as banks does not only attract huge fines for the service providers but also puts customers at risk of being exposed to criminal behaviour. On the other hand, compliance to regulatory requirements (which are necessary to curb crime) is not easy due to several reasons that include the need to do manual and time-consuming audits while at the same time relying on data from traditionally duplicative and siloed data sources.

Resulting from the foregoing, the aggregation of information from previously siloed data sources by blockchain technology will make compliance with regulations automated and unquestionably reliable and quick. ([Microsoft 2018](#)). In fact, Microsoft believes that systems such as Corda cannot only reduce costs of processing information but can significantly curb the occurrence of multiple versions of truths that are associated with manually verified data, much to the chagrin and annoyance of fraudsters who up to now ride on siloed data.

Digital ledger technology is potentially more resilient to cybercrime due to the decentralized nature of the system. In fact, databases that are centralized are easier to attack because there is a central point that can be targeted for paralysis ([International Bank for Reconstruction and Development/ the World Bank 2017](#)). [Liu and Xu \(2019\)](#) argue that in a permissionless blockchain, the bigger the blockchain, the more secure the information in the network. In fact, as the blockchain network grows, the technology would graduate from just being an information system for executing particular transactions of an individual entity to becoming an infrastructure for whole business communities. Again, as the connected community grows, it becomes more and more difficult for individual entities to change the ledger contents ([Liu & Xu, 2019](#)). In view of that [Liu and Xu \(2019\)](#) came up with the model in Figure 2 to demonstrate the link between the business community and the blockchain ledger network.

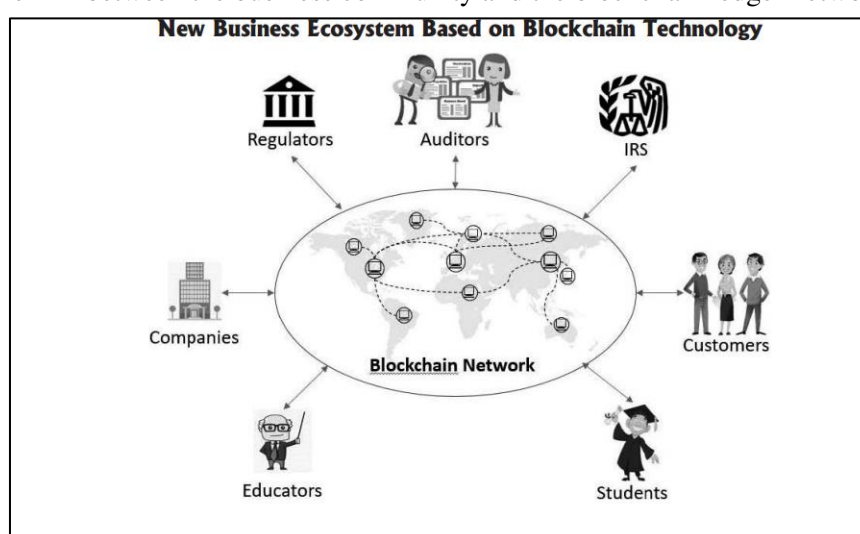


Figure 2. New business ecosystem based on blockchain technology
Source: [Liu and Xu \(2019\)](#)

Thus, informed by the reviewed literature above and inferring from the model by [Liu and Xu \(2019\)](#), the authors came up with the model in Figure 3 in which the removal of third parties, enhanced and efficient know your customer, removal of information silos and reduction of audit costs (all enabled by blockchain ledger technology) are linked to the reduction of financial crimes.

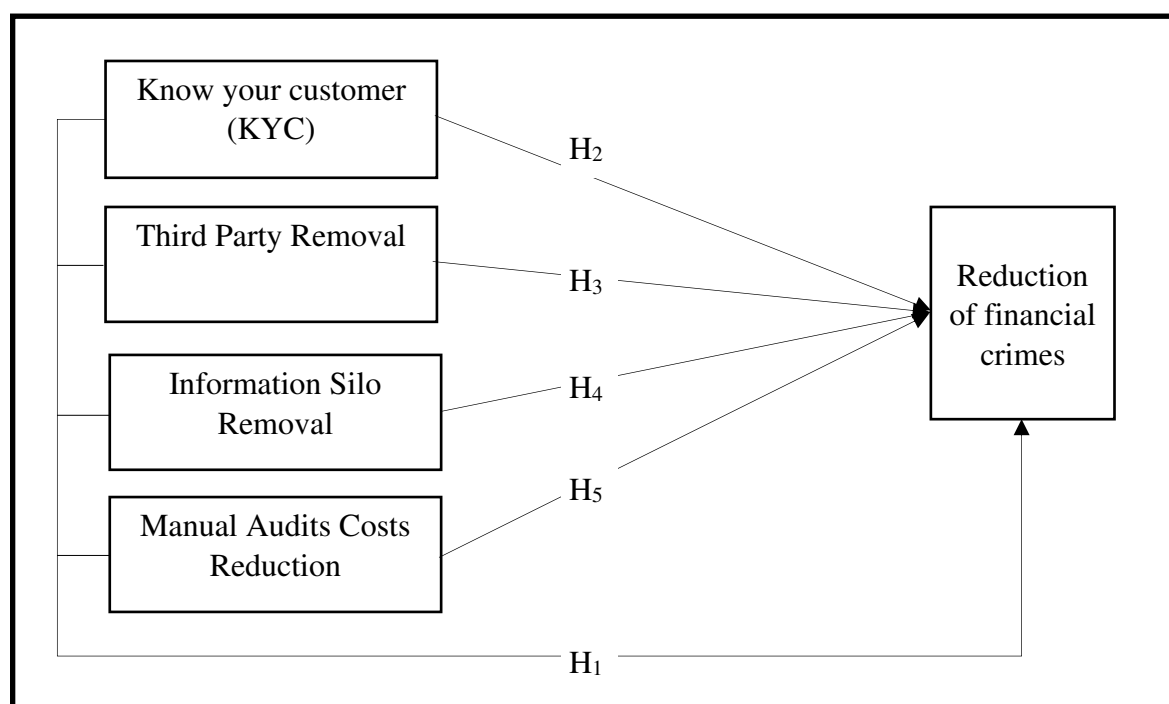


Figure 3. The conceptual framework

The study, therefore, presents the following hypotheses:

H₁: Adoption of blockchain ledger technology positively impacts financial crime reduction

H₂: KYC strategy directly minimizes financial crimes

H₃: Third-party removal positively impacts financial crime reduction

H₄: Removal of information silos positively impacts financial crime reductions

H₅: Reduction of manual audit costs positively impacts financial crime reduction.

3. Research methodology

The study adopted a positivist research philosophy because it validates objective assessments of BCLT and financial crimes. A deductive approach was thus followed which enabled the study to test a theory. The study made use of the survey strategy to collect data. Guided by the positivism research philosophy adopted, the study adopted a quantitative approach in which the study variables were quantified through a structured questionnaire. The target population was made up of financial executives and employees of companies operating in Zimbabwe, senior staff members at the Stock Exchange, bankers, and officials from the financial regulators. The selection of the population was done after the researchers judged that the stock exchange listed companies are the most active players in the financial markets and thus privy to the usage of the latest technology such as blockchain ledger technology. In fact, they are also privy and susceptible to the commission of financial crimes. The study was conducted in an ethical manner as participants in the study did so voluntarily and were made aware of the purpose of the study and the use to which information gathered would be put.

4. Results and discussions

The study managed to attract 182 responses from the sampling frame. The majority (40%) of respondents had post-graduate degrees, followed by 28% with doctoral qualifications, degree (25%) whilst only 7% had a high school qualification. This is an indication that the data was collected from knowledgeable people who could give accurate and reasonable information. With regards to the types

and or forms of financial crimes that are happening on the watch of third parties such as clearing houses, stock exchanges, derivatives exchanges, and central counterparties; the study found out that asset misappropriation was topping the list. The study thus found out that the top ten crimes were asset misappropriation (88%), bribery and corruption (81%), procurement fraud (79%), tax evasion (63%), market manipulation (60%), money laundering (53%), insider trading (48%), pyramid schemes and affinity fraud (44%), cybercrime (41%) and advance fee fraud (40%).

Exploratory factor analysis

The 25 items of the block ledger scale were subjected to principal component analysis (PCA). During the analysis, the correlation matrix was analyzed to verify the presence of inter correlations of 0.3 and above in line with the recommendation of [Pallant \(2005\)](#). This assumption was met and the test was run. The Kaiser-Meyer-Olkin (KMO) value was 0.794 which surpassed the minimum threshold of 0.6 ([Pallant, 2005](#)). At the same time, Bartlett's Test of Sphericity recorded a chi-square value of 1034.71, with a significant P-Value of 0.00 ($P < 0.05$). These two results support the relevance of data for factorability.

Principal component analysis revealed the presence of five components with eigenvalues exceeding 1, explaining 30.39%, 24.78%, 13.54%, 9.01%, and 7.04 of the variance respectively. To further verify the presence of five blockchain factors, the scree plot inspection was done. The scree plot shows a clear break after the fifth component. Guided by Pallant (2005), after a break in the plot, we accept all factors to the left. Using this guiding principle, the study accepted five factors. This means that the principal component analysis has identified the presence of five variables among the study instruments. This was well aligned with the grounded theory and conceptual model adopted which had four blockchain ledger acceptance independent variables and one dependent variable: financial crime reduction. The scree plot also supported the presence of five variables.

To enhance the interpretation of the five blockchain technology factors identified, a robust test statistic called Varimax with Kaiser normalization analysis was performed. The results show that all five blockchain technology factors loaded substantially on five factors. These loadings confirmed the underlying blockchain technology theory that each factor was measured with the respective items. The items loaded were substantially high except for items MAC5, TPR3, and IS4 which loaded below the minimum threshold of 0.50 ([Pallant, 2005](#)). Therefore, in this study, item MAC5 (manual audit costs item 5), TPR 3 (third party removal item 3), and IS4 (information silo) were dropped from further analysis, and the manual audit cost, third part removal, and information silo variables were analyzed with four items each (MAC 1 to 4; TPR 1 to 4; IS1 to 4). The interpretation of these factors was thus in line with the conceptual framework. The four independent variables for the study were therefore confirmed as know your customer (KYC1 to KYC5), manual audit costs (MAC1 to MAC4), third party removal (TPR 1 to 4), and information silos (IS1 to IS4).

Multi collinearity and reliability tests

Table 1. Reliability and collinearity statistics

	Reliability Statistics		Collinearity Statistics	
	Cronbach's Alpha	N of Items	Tolerance	VIF
Manual audit costs	0.800	4	0.769	1.300
Third party removal	0.876	4	0.419	2.385
Information silo	0.748	4	0.457	2.188
Know your customer	0.847	5	0.642	1.557
Financial Crime	0.814	5		

Table 1 presents statistical findings for multicollinearity and reliability of the study variables. The Cronbach Alpha test statistic shows that all variables had a Cronbach Coefficient above 0.74. This proves that all questions under study were measuring their intended variables, meaning the instrument was reliable. [George and Mallery \(2016\)](#) opined that the acceptable values of Cronbach Alpha range between 0.65 and 0.95.

To ascertain the multicollinearity of independent variables, the Variance Inflation Factor (VIF) statistic was computed. It can be noted from Table 1.1 that all VIF values ranged between 1.30 and 2.39. [Shrema \(2020\)](#)'s remarks were used to make a conclusion. According to [Shrema \(2020\)](#) if the VIF values are below 5 then the assumption of multicollinearity would have passed. VIF of above 5 and below 10 require further analysis whilst those above 10 violate the regression assumption. Thus, using the Variance Inflation Factors (VIF) test results above, the model passed the regression assumption and proceeded to the regression analysis and correlation analysis.

The effect of blockchain ledger technology on financial crime reduction

The first hypothesis for the study proposed a positive effect of blockchain ledger technology on financial crime reduction. To test the hypothesis, a stepwise regression method was used. Table 2 presents the model summary.

Table 2. Model Summary

Model Summary									
Model	R	R ²	Adjusted R ²	Std. Error of the Estimate	Change Statistics				
					R ² Change	F Change	df1	df2	Sig. F Change
1	.310 ^a	.096	.091	2.34147	.096	21.294	1	201	.000
2	.577 ^b	.333	.326	2.01584	.237	71.183	1	200	.000
3	.593 ^c	.352	.342	1.99176	.019	5.865	1	199	.016
a. Predictors: (Constant), Know Your Customer									
b. Predictors: (Constant), Know Your Customer, Third Party Removal									
c. Predictors: (Constant), Know Your Customer, Third Party Removal, Information Silo									

Table 2 presents the summary of the three models which emerged from the analysis. Three models are presented with different r-squared values. Model 3 which had three independent variables (Know Your Customer, Third Party Removal, and Information Silo) was adopted for analysis because it explains financial crime reduction by the highest rate of 34% (adjusted $r^2 = 0.342$). Through results presented in Table 2, a significant F change was noticeable from model 2 to 3 ($P = 0.016 < 0.05$), whilst model 3 was also grounded solidly from model 2 by an R^2 change of 0.019. Although the R^2 value for model 3 (0.342) seems relatively low, this is more ideal as financial crime is not only reduced by blockchain ledger technology alone. There are other factors that also determine financial crime other than the ones in the model. However, the study managed to offer substantial evidence of a strong positive association between financial crime reduction and blockchain ledger technology adoption with a correlation coefficient of 0.593. This means that if the variables of the model are enhanced financial crime will be reduced.

Table 3. Analysis of variance statistics

ANOVA ^a						
Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	116.742	1	116.742	21.294	.000 ^b
	Residual	1101.977	201	5.482		
	Total	1218.719	202			
2	Regression	405.999	2	203.000	49.956	.000 ^c
	Residual	812.720	200	4.064		
	Total	1218.719	202			
3	Regression	429.268	3	143.089	36.069	.000 ^d
	Residual	789.452	199	3.967		
	Total	1218.719	202			
a. Dependent Variable: Financial Crime Reduction						
b. Predictors: (Constant), Know Your Customer						
c. Predictors: (Constant), Know Your Customer, Third Party Removal						
d. Predictors: (Constant), Know Your Customer, Third Party Removal, Information Silo						

Table 3 shows the significance level of the identified models. It shows that the blockchain ledger technology model 3 was statistically significant. The p-value of the model was 0.00, with an F coefficient of 36.069. The p-value was below the alpha value of 0.05. Therefore, $p = 0.000 < 0.05$. That means that the model was suitable for analysis with only three independent variables namely know your customer, third party removal and information silo. This supports the *first hypothesis* that the adoption of blockchain ledger technology acts to minimize financial crimes. The same notion is supported in the literature as [Zarpala and Casino \(2020\)](#) also confirm a positive effect of blockchain technology on crime reduction. Furthermore, in support of the current findings, [Polyviou, Velanas, and Soldatos \(2019\)](#) note that crime reduction can be reduced by an effective and efficient Know Your Customer process enabled by blockchain; whilst [Liu & Xu \(2019\)](#) concluded the use of blockchain can significantly free auditors from the traditional evidence gathering activities-and thus leaving them with enough time for performing financial advisory roles

The other fourth variable of the conceptual model (manual audit costs) was discarded from the fit model. The study, therefore, concludes that the adoption of blockchain ledger technology positively impacts financial crime reduction (hypothesis 1). Table 4 shows the blockchain technology coefficients and the level of significance for each determinant. Results in Table 4 were used to accept or reject hypotheses 2 to 5.

Table 4. Blockchain ledger technology coefficients

Coefficients							
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Correlations
		B	Std. Error	Beta			Zero-order
1	(Constant)	14.027	.558		25.135	.000	
	Know your customer	.188	.041	.510	4.615	.000	.710
2	(Constant)	7.599	.901		8.437	.000	
	Know your customer	.355	.040	.585	8.818	.000	.710
	Third party removal	.313	.037	.560	8.437	.000	.672
3	(Constant)	6.736	.959		7.026	.000	
	Know your customer	.366	.040	.604	9.151	.000	.710

Third party removal	.236	.048	.423	4.883	.000	.672
Information silo removal	.148	.061	.202	2.422	.016	.549
a. Dependent Variable: Financial Crime Reduction						

The second hypothesis for the study aimed to test the association between the know your customer strategy and financial crimes. Using model 3 results, the study found out that KYC strategy significantly impacts on financial crime reduction ($\beta = 0.604$, $P = 0.00$, $T = 9.151$, $r = 0.710$). This shows that the adoption of blockchain technology enhances customer experience management through recognition of key customers, that strategy directly and significantly inhibits financial crimes. A strong positive correlation between the two variables of 0.71 also testifies to the high degree of effectiveness of blockchain ledger technology as a tool to enhance customer personalization and financial crime reduction. The study, therefore, concluded that the KYC strategy directly minimizes financial crimes (H_2). The same conclusion was made by the [International Finance Corporation \(2017\)](#) which indicates that high crime rates associated with duplication of names by financial institutions can also be done away with through KYC strategy as blockchain technology infuse the process in an authentic manner. Conversely, the [Harvard Law School \(2020\)](#) also concluded that the costs and crimes by banks in vetting new customers who want to open accounts can be drastically reduced or done away with completely through the adoption of blockchain technology.

The third hypothesis tested the proposition that third-party removal positively impacts financial crime reduction. Using Table 4 results, that association was accepted with a significant p-value of 0.000, a standardized beta coefficient of 0.423 with a T-value of 4.883. The correlation statistics also confirmed a strong positive association between third-party removal and financial crime reduction ($r = 0.672$, $P = 0.00$). Thus, we interpret that adoption of the block ledger digital technologies through third-party removal significantly eradicates financial crimes by a factor of 42%. As more and more financial institutions adopt blockchain technology and third-party removal, financial crimes will significantly be reduced. DBS Group research (2016), supports the removal of third parties in financial transactions by digital ledger technology. Their argument is that the data concentrated on the third party entices internal and external hackers. The same notion was supported by other researchers ([Hanni & Kalin, 2013](#); [Statista, 2021](#)).

The fourth hypothesis aimed to assess the role of blockchain technology in reducing financial crimes through the removal of information silos. The alternate hypothesis was accepted ($\beta = 0.20$, $T = 2.422$, $P = 0.016$, $r = 0.549$). this therefore follows gives evidence that the adoption of blockchain technology enhances the removal of information silos. Statistics herein have proved that the removal of information silos significantly contributes to the reduction of financial crimes by a factor of 20%. In that same line of argument, [Microsoft \(2018\)](#) stated that blockchain technology can reduce the cost of processing information and reduce the risks of financial crimes as digitalized information about transacting parties will be in digital lockers for all to see. [Niforos \(2017\)](#) further indicates that the aggregation of information from previously siloed data sources by blockchain technology will make compliance to regulations automated and unquestionably reliable and quick thereby reducing financial crimes.

The conceptual model for this study had a fourth independent variable for blockchain technology, manual auditing costs. The study however found out that the variable was not statistically significantly explaining the reduction of financial crimes. Therefore, the manual auditing cost variable was dropped from analysis using stepwise regression. Table 5 shows the results of the excluded variable.

Table 5. Variable excluded from the blockchain technology model

Excluded Variables^a				
Model		Beta In	T	Sig.
3	Manual audit costs	-.051 ^d	-.782	.435
a. Dependent Variable: Financial Crime Reduction				
d. Predictors in the Model: (Constant), Know your customer, Third party removal, Information silo removal				

Table 5 shows that the adoption of blockchain ledger technology will not significantly reduce financial crimes through a reduction in manual auditing costs ($\beta = -0.051$, $T = -0.782$, $P = 0.435$). The study, therefore, accepts the null hypothesis and concludes that the adoption of block ledger technology does not reduce financial crimes through a reduction in manual auditing costs. The study found contradictory findings from the ones from the [International Finance Corporation \(2017\)](#) as the Corporation notes that using distributed ledger technology to store financial information can eliminate errors associated with manual auditing, improve efficiency, reduce reporting costs, and potentially support deeper regulatory oversight in the future.

5. Conclusion

The study concluded that blockchain technology adoption is worthwhile for the minimization of financial crimes. Adoption of blockchain ledger technology positively impacts financial crime reduction by a factor of 34%. The conceptual model of the study had four blockchain variables. However, the study concluded that only three of the four variables are statistically significantly explaining financial crime reductions. The significant variables are knowing your customer, third-party removal, and information silo removal. An insignificant association was observed from the association between manual auditing costs and financial crime reduction. Therefore, the study concludes that the blockchain adoption model should be maintained with only three independent variables, as the fourth was discarded.

The research further concluded that as long as the adoption of the blockchain ledger technology is undertaken simultaneously with the amendment of existing laws and formulation of new laws to govern both the use of the technology and the formulation of codes and algorithms that make it work, the global community will effectively and efficiently benefit from capabilities of blockchain ledger technology to significantly reduce some financial crimes that we know today.

The study, therefore, recommends that the adoption of blockchain ledger technology should be undertaken by government departments, private companies, and financial institutions to assist in the reduction of financial crimes. Governments and other financial regulators should craft new laws and amend existing ones if ever the full benefits of adopting blockchain ledger technology in as far as reduction of financial crimes are concerned. Regulation of the coding and formulation of algorithms should be done by governments- lest programmers will take over the roles of legislatures and begin (through coding) to make their laws that regulate financial markets. These recommendations border on the findings in this study that blockchain digital technologies are effective in minimizing financial crimes through enhanced know your customer, third-party removal, and information silo removal.

Limitations and study forward

The study was conducted on financial executives, senior staff members at the stock exchange, bankers, and officials from the financial regulators; hence the results cannot be universal to other categories. A further study on the nexus between blockchain digital ledger technology and financial crimes may also be performed using a different set of methodology. Additionally, conceptual model variables may also be employed to identify the relationship under consideration in this study.

References

- British Bankers' Association. (2015). Future Financial Crime Risks-Considering the financial crime challenges faced by UK banks. Lexis Nexis, Britain.
- European Parliament. (2018). Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion. European Parliament.
- George, D., & Mallery, P. (2016). IBM SPSS statistics step by step: A simple guide and reference. 14th edition. New York, Routledge. Doi:10.4324/9781315545899.
- Gilmore, L. (2017). Reinventing the World of Banking. McKinsey Inc, Bucharest, Romania.
- Gottschalk, P. (2010). Categories of Financial crime. *Journal of Financial Crime*, 17(4), 441 - 458.
- Hanni, L., & Kalin, E. (2013). *Stock Market Offenses and Abuse*, Zurich.
- Harvard Law School. (2020). Anti-Money Laundering and Blockchain Technology. Harvard University, Cambridge, USA.
- Huang, C., & Trangle, A. (2020). Anti-Money Laundering and Blockchain Technology. Harvard University, Cambridge, USA.
- International Bank for Reconstruction and Development/ the World Bank. (2017). Distributed Ledger Technology (DLT) and Blockchain.
- International Federation of Accountants (IFAC), (2018). Blockchain: Impact on Business, Finance and Accounting. Global Knowledge Gateway, IFAC.
- International Finance Corporation. (2021). Blockchain: Opportunities for Private Enterprises in Emerging Markets. IFC, World Bank Group.
- International Finance Corporation. (2017). Blockchain in Financial Services in Emerging Markets. IFC, World Bank Group.
- International Finance Corporation. (2017). Blockchain Opportunities for private Enterprises in Emerging Markets. IFC, World Bank Group.
- International Monetary Fund. (2021). Fight-Against-Money-Laundering-the-Financing-of-Terrorism. IMF Publication.
- INTERPOL. (2021). Crimes/Financial-crime. Interpol International.
- Jung, J., & Lee, J. (2017). Contemporary Financial Crime. *Journal of Public Administration and Governance*, 7(2), 88-97.
- Liu, M. & Xu, J. (2019). How will blockchain technology impact auditing and accounting: permissionless versus permissioned blockchain. American Accounting Association, America
- Mantelaers, E., Zoet, M. & Smit, K. (2019). The impact of blockchain on the auditor's audit approach. *International Journal of Software and e-Business*.
- Microsoft, (2018). 5 Ways Blockchain is Transforming Financial Services, A new approach to brokering trust. Microsoft.
- Niforos, M. (2017). Blockchain in Financial Services in Emerging Markets-Current Trends. IFC, World Bank Group.
- Pallant, J. (2005). SPSS survival guide: A step by step guide to data analysis using SPSS for windows. 3rd Edition. Open university Press, New York.
- KPMG. (2018). Clarity on Financial Crime in Banking Part I: Current Trends. KPMG, Switzerland
- Polyviou, A., Velanas, P., & Soldatos, J. (2019). Blockchain Technology: Financial Sector Applications Beyond Cryptocurrencies. MDPI, Basel, Switzerland.
- Rawat, D. B., & Doku, R. (2020). Blockchain technology: emerging applications and use cases for secure and trustworthy smart systems. *Journal of Cybersecurity and Privacy*, 1, 4 – 18.
- Rigsby, J. H. (2016). Virtual Currency, Blockchain Technology, and EU Law: The "Next Internet" in AML/CFT Regulation's Shadow. Lund University
- SestremOchôa, I., Reis, V., Calbusch, L., De Paz Santana, J., DelcioParreira, W., OriolSeman, L., & Zeferino, C. (2021). Performance and Security Evaluation on a Blockchain Architecture for License Plate Recognition Systems. *Appl. Sci.*, 11(1), 1-20.
- Shrema, N. (2020). Detecting multicollinearity on regression analysis. *American Journal of Applied Mathematics and Statistics*, 8(2), 39-42. Doi:10.12691/ajams-8-2-1.
- Statista. (2021). Types of economic crime reported worldwide in 2016. Statista Research Department, Switzerland.
- UK's Financial Services and Markets Act. (2000). London, UK.

- United Nations Office on Drugs and Crime (2005). *Crime and Development in Africa*. United Nations.
- United Nations Office on Drugs and Crime. (2021). United Nations Office on Drugs and Crime. <https://dataunodc.un.org/data/crime/fraud>
- Violeta, A. M., Vaidean, V. L., Borlea, S. N., & Florescu, D. R. (2021). The Impact of the Development of Society on Economic and Financial Crime. Case Study for European Union Member States. *Risks*, 97, 1-20.
- Wadey. E. (2019). *A-Z of Financial Crime in Africa: The What, Why and How to Tackling Financial Crime in Africa*. Temenos, Netguardians.
- Zarpala. L., & Casino. F. (2020). A Blockchain-Based Forensic Model for Financial Crime Investigation: The Embezzlement Scenario. *Digital Finance Journal*. Doi.org/10.1007/s42521-021-00035-5.