Anonymity And Trust Roles In The Digital Barter Age

Digital Transformation Framework And Digital Assets Popularity Assessment

Alessio Faccia
University of Birmingham Dubai, Dubai, United Arab Emirates; Centre for Blockchain Technologies, University College London, London, United Kingdom
a.faccia@bham.ac.uk

Francesco Manni
Università Roma TRE, Rome, Italy,
francesco.manni@uniroma3.it

Ahmed Eltweri
Liverpool John Moores University, Liverpool, United Kingdom
A.M.Eltweri@ljmu.ac.uk

Luigi Pio Leonardo Cavaliere
università di Foggia Foggia, Italy
luigi.cavalie@gmail.com

Vishal Pandey
Jindal Global Business School O.P. Jindal Global University (JGU), Sonipat, Haryana, India
vpandey@jgu.edu.in

ABSTRACT

Anonymity is generally a controversial feature that presents multiple trade-offs. It preserves privacy but cannot be audited; it ensures voice to the voiceless but is prone to online abuse; it allows whistleblowing, but the information cannot be trusted. It is equally questionable when referring to digital/crypto assets. Depending on the perspectives, it might positively and/or negatively affect digital transformation strategies. This paper's first novelty resides in the original approach to analysing the anonymity and trust roles in electronic commerce transactions from the different stakeholders' perspectives. A basic but solid framework for consistent digital transformation is presented. It is designed to help decision-makers, policymakers, entrepreneurs and engineers. The authors' innovative assumption is that tokens and crypto-assets (including the so-called crypto-currencies) should be considered early forms of digital barter, easily substituted in the future. Another assumption is that bartering is the old/new frontier for illegal activities. Current forms of money are not free from pitfalls. It can be demonstrated by the fact that money laundering activities are evergreen and constantly change channels and techniques. Hence, the focus should be on adequately designed digital infrastructures to ensure the same level of trust currently granted to FIAT currencies and physical assets. Physical Assets Bartering is the most basic form of exchange. Money added (at least) two important functions: unit of account and store of value. Money popularity is linked to governments' public trust and facilitated exchanges. However, it does not mean it is the absolute best form of bartering.

ICSEB 2022, December 09–11, 2022, Shenzhen, China

ACM ISBN 979-8-4007-0009-5/22/12…$15.00
https://doi.org/10.1145/3578997.3579010

CCS CONCEPTS

• **: Applied computing** → Multi-criterion optimization and decision-making.

KEYWORDS

Anonymity, Trust, Digital Barter, Money Laundering, Privacy, Blockchain, Audit trail, NFT, Crypto-asset, Cryptocurrencies

ACM Reference Format:
Alessio Faccia, Francesco Manni, Ahmed Eltweri, Luigi Pio Leonardo Cavaliere, and Vishal Pandey. 2022. Anonymity And Trust Roles In The Digital Barter Age: Digital Transformation Framework And Digital Assets Popularity Assessment. In *2022 6th International Conference on Software and e-Business (ICSEB 2022), December 09–11, 2022, Shenzhen, China.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3578997.3579010

1 INTRODUCTION

Digital identity [1] should limit illegal online activities and transactions since it improves audit trail and responsible behaviour due to the consequences of criminal offences [2]. However, it also generates mass surveillance [3]. Therefore, finding an appropriate balance between personal privacy and other parties' rights is urgent to ensure a fair rule of law.

Digital Identity is considered a right for every European Union (EU) citizen [4]. Not surprisingly, the European digital identity is a concrete legislative proposal under consideration by the bodies of the Union [5, 6]. Every citizen should rely on digital Identity protection, using suitable technology to manage what data is used and how.

Transparency [7] on the use of data by a business or social media platforms is required to ensure public trust [8], and the prevention of online crimes becomes a priority as it impacts the economy. Digital identity could speed up relations with the public administration and is the minimum logical-legal premise to allow online political voting. The use of transparent cryptocurrencies would also positively impact the traceability of exchanges and reduce their appeal. The EU regulators concluded that digital identity is welcome,

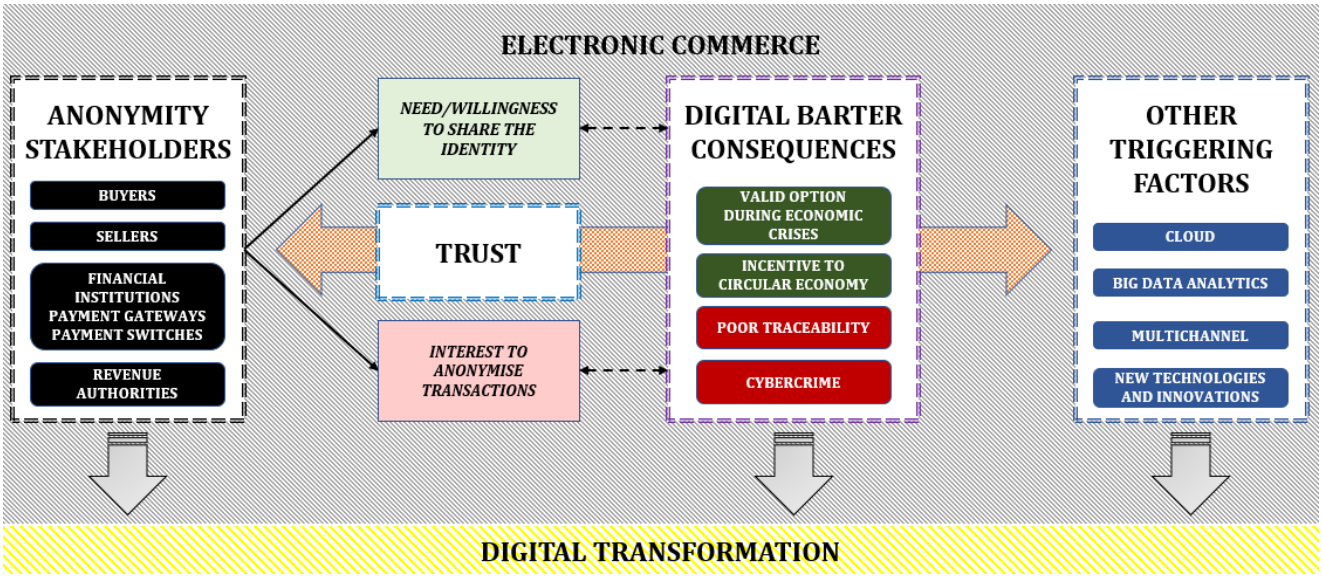

Figure 1: Research Framework.

but online anonymity also deserves protection because it ensures freedom and democracy [9].

Access to social networks is granted upon registration. Email address, mobile number, and nickname are required. Some people use their real names, while others enter a fake or pseudonym. Fake accounts are created this way, allowing people to act anonymously for various reasons. For example, some do not want to be recognised by others or because they want to express their opinion without being judged personally. The web, if used incorrectly, can be very dangerous, favouring cyberbullying, sextortion, paedophilia, fake news and many other dysfunctional behaviours [10, 11].

This research investigates the root causes that contributed to digital assets bartering popularity. Among them, anonymity and trust proved essential key factors determining their growth.

2 RESEARCH FRAMEWORK, RESEARCH HYPOTHESIS AND RESEARCH QUESTIONS

Two main hypotheses are formulated in this research based on the assumption that anonymity and trust are controversial digital asset features [12]. Hence it is necessary to investigate its advantages and pitfalls from different stakeholders' perspectives. A concise review of the essential review of the existing literature was performed to identify the stakeholders' rationale for either welcoming or avoiding digital identification. The authors believe this step did not deserve a formal systematic review as it is only prodromic and introductory to the main following research question.

"*Do anonymity and trust contribute to digital assets' bartering popularity?*". This research question is addressed by implementing and modelling a framework that matches stakeholders' needs and potential outcomes. Mitigating strategies are also suggested to policymakers [13]. Each association is made through the application of deductive reasoning.

This research followed the research framework presented in Figure 1.

3 FINDINGS

3.1 Potential anonymity stakeholders in the electronic commerce transactions

Undoubtedly electronic commerce involves many entities (IT and IS providers) and various players in the performance of a commercial transaction [14]. The most relevant recurring stakeholders in this context are sellers, buyers, financial institutions, payment gateways, payment switches, and revenue authorities. Below, their perspectives and interests ("stakes") are considered regarding the transaction anonymity:

- Buyers are the most interested in hiding their identity for tax purposes (based on consumptions and investments) or because they are unwilling to have their purchasing behaviours tracked. The only reason they might prefer their identity to be disclosed is to ensure that a specific (important) purchase of registered assets (i.e., vehicles, real estate) can be associated with them for further sales [15, 16].
- Sellers share rationales similar to the buyers as their sales increase their taxable income, and they would like to avoid sharing their financials with their competitors. However, they are interested in tracking their customers' purchasing behaviours, feeding their systems big data to perform good analytics.
- Financial institutions, payment gateways and switches, are increasingly witnessing a growing revenue share from their valuable big data [17], and they have no interest in ensuring transaction anonymity apart from regulatory requirements (i.e., GDPR) or against their competitors.

Table 1: Anonymity and its main stakeholders' perspectives

Stakeholders	Interest to anonymise transactions	Need / Willingness to share the identity
Buyers	✓Tax evasion/avoidance ✓Illegal/immoral transactions ✓Avoid purchasing behaviour tracking	x Purchase of registered assets (i.e., vehicles or real estate)
Sellers	✓Tax evasion/avoidance ✓Hiding analytics from competitors	x Tracking customers' purchasing behaviours
Financial Institutions Payment Gateways Payment Switches	✓Internal Data Mining Analytics	x Regulatory requirements
Revenue Authorities	✓Taxpayers' privacy	x Prevent tax evasion/avoidance

- Revenue authorities are the most interested in gathering identity data of all the parties involved in e-commerce transactions to prevent tax evasion [18]. See Table 1 below.

3.2 Digital Barter origins and consequences

Barter is the most basic form of trade. Any transaction can be performed through goods exchanges. Digital bartering is a specific form of barter that involves the exchange of digital (intangible) assets. Compared to traditional (physical) bartering, it is much more efficient, being instant, achievable worldwide (through the Internet), frictionless, and (sometimes) anonymous [19]. In most cases, the parties involved in the transaction do not know each other and are not interested in sharing their identities.

Over time, many forms of assets have become popular to facilitate transactions. Namely, money (in the form of coins and banknotes) was the first to be trusted (issued by reputable public institutions) and used. The three well-known functions of money (store of value, unit of account, and medium of exchange) [20] contributed to their popularity, as every single coin or banknote is perfectly fungible and easily exchanged. In modern times, physical money is being replaced by digital FIAT money, commercial bank money and, very soon, by Central Bank Digital Currencies (CBDCs), thanks to projects piloted in many countries [21].

Parallelly, we are witnessing increasing volumes of other digital asset exchanges. Among them are crypto-currencies and Non-Fungible Tokens (NFTs). Volatility is their source of joy and torment [22, 23]. It facilitates speculation but cannot ensure the store of the value function. Apart from this weakness, it is possible to state that digital assets unbacked by governments share most of the physical money characteristics and, in some cases, are even better substitutes. They can be easily exchanged. Specifically, cryptocurrencies are fungible (their hash is unique, but their value is traded independently), and NFTs, although non-fungible (by nature), like cryptocurrencies, ensure proof of ownership through the blockchain. By comparing the above features, it appears clear why governments and central banks are so concerned by unbacked assets diffusion.

Table 2 demonstrates how, in substance, cryptocurrencies and NFTs are now popular, ensuring trust. Indeed, although unbacked by Central Banks, they can be considered good substitutes for physical money. Although their volatility, they share one important feature with coins and banknotes: anonymity.

Given the above assumptions, the increasing popularity of digital bartering is not surprising. It proved very efficient and appealing during the Covid pandemic and the subsequent economic crisis. It supports circular economy practice through digital backbone exploitation [24]. However, it favoured, like physical money in the past, illegal trade and money laundering, and it is prone to cybercrimes (i.e., phishing and ransomware) [25, 26].

3.3 The ambiguous role of trust: a criminal perspective

Focusing again on Table 2 findings, it is evident that Cryptocurrencies and NFTs share very similar characteristics with physical currencies. Anonymity is their main advantage from a criminal's perspective. Indeed, from this point of view, digital assets are even more efficient than physical money since they can be transferred instantly, with zero audit trail.

The Nigerian experience of the e-Naira, the local CBDC, demonstrated that despite the noble intent of the Central Bank to support financial inclusion and challenge the cryptocurrency popularity, miserably failed so far [27].

We could have expected higher trust in a Central Bank rather than unbacked digital assets. However, this is not the case. It is reasonable to suggest that the technology or the centralised support of reputable institutions are not among the main influencing factors.

Fintech illiteracy [28] also played an important role in this outcome since only very few know the difference between CBDCs (backed) and Cryptocurrencies (unbacked). Therefore, international cryptocurrency popularity most probably was determinant. Alternatively, the only other feature differentiating CBDCs from Cryptocurrencies is anonymity. The latter facilitates untracked transactions with fungible (although volatile) intangible digital assets. Moreover, given the declining use of physical currencies, we can reasonably consider that most illegal transactions might have been anonymously bartered through cryptocurrencies or NFTs (the only anonymous alternatives, differently than e-money, commercial

Table 2: Cryptocurrencies, NFTs, Coins and Banknotes, Commercial Bank Digital Currency, CBDCs

	Cryptocurrencies	NFTs	Coins and Banknotes	Commercial Bank Digital Currency	CBDCs
Fungibility	YES	NO	YES	YES	YES
Unit of Account	YES	NO	YES	YES	YES
Trust Mechanism	Diffused	Diffused	Centralised	Centralised	Centralised
Central Bank Role	Unbacked by CB	Unbacked by CB	Issued by CB	Backed by CB to a limited extent	Issued by CB
Technology	Blockchain	Blockchain	Physical	Centralised	Centralised/Blockchain
Volatility	HIGH	HIGH	Low (depending on currency)	Low (depending on currency)	Low (depending on currency)
Anonymity	YES	YES	YES	NO	YES/NO
Medium of Exchange	YES	YES	YES	YES	YES

bank money and CBDC). It is no coincidence that bitcoins are the preferred currency on the dark web [25, 29].

Moreover, public authorities demonstrated limited effectiveness in preventing the use of digital assets to perform transactions [30]. Moreover, even if they prove successful, internet users can easily switch (and trust) to ever-new digital assets with similar characteristics that will initially run unnoticed.

Another element to identify digital assets potentially targeted as trusted by criminals for their transactions is the high value they can carry, allowing fewer transactions to minimise the risk of being noticed. From this perspective, it is justified that the high price is attributed to the most popular "cryptos" (i.e., Bitcoin) or some NFTs. In the physical world, bartered goods that usually played similar roles have been Rolex watches, diamonds, and gold that can be easily carried/worn and exchanged at the time of the (potentially illegal) transaction [31, 32]. As in any barter, it is sufficient that two parties agree on a value to perform the transaction. In the case of digital assets, despite their volatility, the price at the time of the transaction can be specifically identified. Whatever the change in price, it can still be considered in "acceptable ranges", and the risk of using any other physical alternative is much higher than the risk of sudden devaluation of the agreed digital assets.

Ultimately, it is unquestionable that the value of exchange (conversely than the value in use, which in the crypto-currencies is virtually non-existent) is based on trust and popularity. Notwithstanding, Commercial Bank Digital Currencies are not entirely safe (since Central Banks back them to a limited extent), but they are still trusted. Similarly, to extreme extents, Central Banks cannot rely on unlimited funds, and almost none of the countries are debt-free. Therefore, their insolvency risk is never considered absolutely absent or truly risk-free.

3.4 Other Triggering Factors

Consequently, effective digital transformation strategies to be enforced in Electronic Commerce should a) rely on public trust, b) be limited to legitimate activities; but also, c) be seamless, and d) ensure an adequate level of privacy and fairness.

The requirements mentioned above are often conflicting, however equally relevant. Apart from the previously mentioned consequences and perspectives when it comes to anonymity and trust in digital barter, other factors are currently triggering a digital transformation in e-commerce, namely:

1. Use of cloud technologies that facilitate ubiquitous transactions, communications, and data storage;

2. Big data analytics that turned into even more valuable transaction digitalisation [33];

3. Multichannel opportunities that allow interoperability, ensuring instant payments locally, cross-border, and using a wide range of different gateways, currencies, technologies and third-party payment systems;

4. New technologies and fintech innovations facilitate transactions outside traditional (heavy-regulated) financial services.

Moreover, the design of the platforms, centralised or decentralised, plays a pivotal role in the successful implementation of safe environments and fosters innovation [34].

Therefore, implementing feasible and safe digital transformation strategies is challenging from a policymaker perspective. The framework proposed in Figure 2 presents a holistic perspective that considers the combination of trust and anonymity concerning the shift from a cash society/traditional trade to cashless society/digital barter.

The evidence shows that buyers' and sellers' benefits are prevailing, and their trust is shifting from Central Banks to Digital Technologies. The increasing use of Digital Assets demonstrates this, regardless of whether they are unbacked by Central Banks. Among the drivers determining this paradigm shift, the need for anonymity can be associated with positive (Purchasing Behaviour Tracking Avoidance) or blameful (Tax Evasion/Avoidance or Illegal/Immoral Transactions) root causes. Given that digital transformation is irreversible, there is an urgent need for revenue authorities, regulators, and forensic analysts to improve their tools to prevent illegal trade in alternative ways than relying on payments monitoring.

Even though consumers' privacy might appear less important than preventing illegal trade or money laundering, digital assets engineering is nimble, and the trust in digital technologies is so strong that it is too easy to be limited.

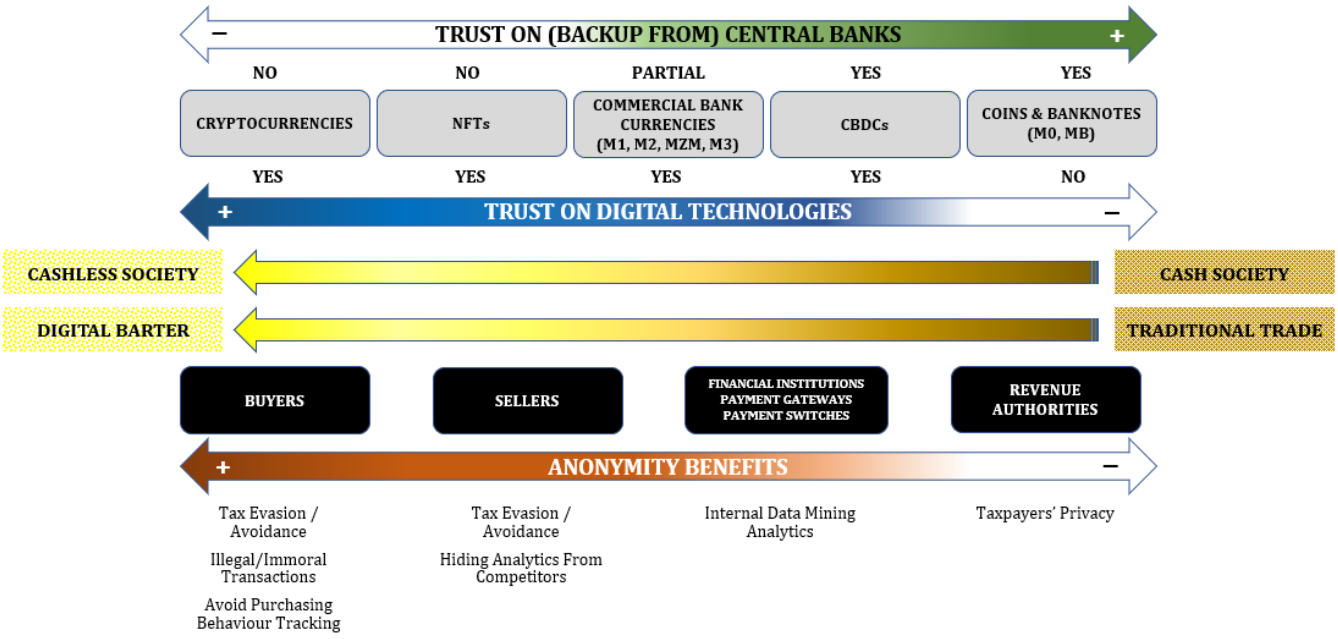

Figure 2: Anonymity and Trust Analysis Framework

4 CONCLUSIONS

This research focused on two crucial aspects that proved essential for the growing digital assets' popularity. Digital assets, in their most trendy forms of Cryptocurrencies and NFTs, are now popular because they are still not subject to taxation and are anonymous. Their trendy popularity is still allowing them to store high value. The above features (anonymity, similar to paper money and high-value store, similar to diamonds, Rolex watches or gold) combined are a perfect mix for criminals who intend to launder money or to perform illegal transactions that also benefit from seamless transactions.

The framework presented in Figure 2 analyse these factors and further confirms this, so far, irreversible trend, where not even the Central Banks can compete in terms of the trust. Policymakers should seriously consider the factors mentioned above and challenge illegal bartering at its roots instead of targeting payment methods or transactions. Indeed, in the digital era, digital barter proved so nimble that the players can adapt to changes instantly and trust alternative (always new) digital assets when some are banned, taxed or limited. The recent IRS attempt might have been, for example, more generic and principle-based by referring to "digital assets" in general instead of making specific reference to tax "Cryptocurrencies" and "NFTs" [35]. Consequently, as per the above assumptions, we can soon expect the rise of new, alternative, high-valued, anonymous digital assets to lead the digital barter.

REFERENCES

[1] Masiero, S. and Bailur, S., 2021. Digital identity for development: The quest for justice and a research agenda. Information Technology for Development, 27(1), pp.1-12.
[2] Weitzberg, K., Cheesman, M., Martin, A. and Schoemaker, E., 2021. Between surveillance and recognition: Rethinking digital identity in aid. Big Data & Society, 8(1), p.20539517211006744.
[3] Feher, K., 2021. Digital identity and the online self: Footprint strategies–An exploratory and comparative research study. Journal of information science, 47(2), pp.192-205.
[4] Rieger, A., Roth, T., Sedlmeir, J., Weigl, L. and Fridgen, G., 2022. Not yet another digital identity. Nature Human Behaviour, 6(1), pp.3-3.
[5] Codagnone, C., Liva, G. and de las Heras Ballell, T.R., 2022. Identification and assessment of existing and draft EU legislation in the digital field. Study for the Special Committee on Artificial Intelligence in a Digital Age (AIDA). Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg.
[6] Sedlmeir, J., Smethurst, R., Rieger, A. and Fridgen, G., 2021. Digital identities and verifiable credentials. Business & Information Systems Engineering, 63(5), pp.603-613.
[7] Kempeneer, S., 2021. A big data state of mind: Epistemological challenges to accountability and transparency in data-driven regulation. Government Information Quarterly, 38(3), p.101578.
[8] Felzmann, H., Villaronga, E.F., Lutz, C. and Tamò-Larrieux, A., 2019. Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns. Big Data & Society, 6(1), p.2053951719860542.
[9] Sardá, T., Natale, S., Sotirakopoulos, N. and Monaghan, M., 2019. Understanding online anonymity. Media, Culture & Society, 41(4), pp.557-564.
[10] Moore, A., 2018. Anonymity, pseudonymity, and deliberation: Why not everything should be connected. Journal of Political Philosophy, 26(2), pp.169-192.
[11] De La Hoz, G.T., 2021. New Trends in Online Crime Using Social Networking Sites and Apps against Children and Adolescents: Police-Based Longitudinal Research. International Journal of Cyber Criminology, 15(1), pp.31-49.
[12] Grinyaev, S.N., Zlotin, R.A., Milushkin, A.I., Pravikov, D.I., Selionov, I.A., Shcherbakov, A.Y. and Shchuko, Y.N., 2018. On the Creation of a Universal Protected Trusted Digital Asset (Token). Automatic Documentation and Mathematical Linguistics, 52(5), pp.265-273.
[13] Khalilov, M.C.K. and Levi, A., 2018. A survey on anonymity and privacy in bitcoin-like digital cash systems. IEEE Communications Surveys & Tutorials, 20(3), pp.2543-2585.
[14] Chua, C.E.H., Straub, D.W., Khoo, H.M. and Kadiyala, S., 2005. The evolution of e-commerce research: A stakeholder perspective. Journal of Electronic Commerce Research, 6(4).
[15] Aldridge, J., 2019. Does online anonymity boost illegal market trading?. Media, Culture & Society, 41(4), pp.578-583.
[16] Phelps, A. and Watt, A., 2014. I shop online–recreationally! Internet anonymity and Silk Road enabling drug use in Australia. Digital Investigation, 11(4), pp.261-272.
[17] Tao, H., Bhuiyan, M.Z.A., Rahman, M.A., Wang, G., Wang, T., Ahmed, M.M. and Li, J., 2019. Economic perspective analysis of protecting big data security and

privacy. Future Generation Computer Systems, 98, pp.660-671.
[18] Alm, J., 2021. Tax evasion, technology, and inequality. Economics of Governance, 22(4), pp.321-343.
[19] Anbugeetha, D. and NANDHINI, B., 2021. EVOLUTION OF MONEY: FROM BARTER SYSTEM TO DIGITAL MONEY. The New Era of Digital Payments, p.55.
[20] Mattke, J., Maier, C. and Reis, L., 2020, June. Is cryptocurrency money? Three empirical studies analysing medium of exchange, store of value and unit of account. In Proceedings of the 2020 on Computers and People Research Conference (pp. 26-35).
[21] Morales-Resendiz, R., Ponce, J., Picardo, P., Velasco, A., Chen, B., Sanz, L., Guiborg, G., Segendorff, B., Vasquez, J.L., Arroyo, J. and Aguirre, I., 2021. Implementing a retail CBDC: Lessons learned and key insights. Latin American Journal of Central Banking, 2(1), p.100022.
[22] Ghorbel, A. and Jeribi, A., 2021. Investigating the relationship between volatilities of cryptocurrencies and other financial assets. Decisions in Economics and Finance, 44(2), pp.817-843.
[23] Faccia, A. and Petratos, P., 2021. Blockchain, enterprise resource planning (ERP) and accounting information systems (AIS): Research on e-procurement and system integration. Applied Sciences, 11(15), p.6792.
[24] Pagoropoulos, A., Pigosso, D.C. and McAloone, T.C., 2017. The emergent role of digital technologies in the Circular Economy: A review. Procedia CIRP, 64, pp.19-24.
[25] Faccia, A., Moşteanu, N.R., Cavaliere, L.P.L. and Mataruna-Dos-Santos, L.J., 2020, September. Electronic money laundering, the dark side of fintech: An overview of the most recent cases. In Proceedings of the 2020 12th international conference on information management and engineering (pp. 29-34).
[26] Petratos, P. and Faccia, A., 2019, August. Accounting information systems and system of systems: Assessing security with attack surface methodology. In Proceedings of the 2019 3rd International Conference on Cloud and Big Data Computing (pp. 100-105).
[27] Osae-Brown, A., Fatunde, M. and Olurounbi, R. 2022. Digital-Currency Plan Falters as Nigerians Defiant on Crypto. Bloomberg. Available at https://www.bloomberg.com/news/articles/2022-10-25/shunned-digital-currency-looks-for-street-credibility-in-nigeria?leadSource=uverify%20wall.
[28] Ozili, P.K., 2022. Central bank digital currency in Nigeria: opportunities and risks. In The New Digital Era: Digitalisation, Emerging Risks and Opportunities (Vol. 109, pp. 125-133). Emerald Publishing Limited.
[29] Piazza, F., 2016. Bitcoin in the dark web: a shadow over banking secrecy and a call for global response. S. Cal. Interdisc. LJ, 26, p.521.
[30] Mosteanu, N.R. and Faccia, A., 2020. Digital systems and new challenges of financial management–FinTech, XBRL, blockchain and cryptocurrencies. Quality-Access to Success Journal, 21(174), pp.159-166.
[31] Haken, J., 2011. Transnational crime in the developing world. Global financial integrity, 32(2), pp.11-30.
[32] Gilmour, N., 2017. Blindingly obvious and frequently exploitable: Money laundering through the purchasing of high-value portable commodities. Journal of Money Laundering Control.
[33] Faccia, A., Cavaliere, L.P.L., Petratos, P. and Mosteanu, N.R., 2022, August. Unstructured Over Structured, Big Data Analytics and Applications In Accounting and Management. In Proceedings of the 2022 6th International Conference on Cloud and Big Data Computing (pp. 37-41)..
[34] Faccia, A., Pandey, V. and Banga, C., 2022. Is permissioned blockchain the key to support the external audit shift to entirely open innovation paradigm?. Journal of Open Innovation: Technology, Market, and Complexity, 8(2), p.85.
[35] Slowey, E. 2022. The IRS is Making It Easier To File Your Crypto Taxes. Bloomberg. Available at: https://www.bloomberg.com/news/articles/2022-10-18/crypto-investors-get-some-answers-in-us-tax-form-instructions?leadSource=uverify%20wall