Fintech Digital Products and Customer Consent- Ontrust solution

Author Name: Manoj Babu Devapathni Yugandhar
Role and Affiliation: Solution Architect,Wintrust financial
Address: Wellspring dr lithia FL, USA
Email: dymanojbabu@gmail.com

Abstract- The entire study has explored the whole impact of Ontrust solutions in enhancing the customer's consent management and compliance in services of fintech. This examines how fintech platformers can streamline the whole process, ensuring transparency, security, and some adherence like GDPR, PSD2, CCPA, etc. Ontrust leverages blockchain for tamper-proof consent which has recorded an AI of detection for fraud and improves customer satisfaction. The research investigates the roles of these technologies in overcoming challenges like non-compliance, and data privacy risk. In the results section, the growth of fintech-based technology adoption has been highlighted and other segments like startup investments, demographic trust difference, and consent solution security compliance have also been analysed. The study provides insights into best practices and future development in digital consent solutions for financial institutions.

Index Terms- Fintech, Consent Management, Blockchain, AI, Regulatory Compliance

I. INTRODUCTION

A. Background to the Study

The rapid digital transformation of financial services has aroused the fintech solutions switch and enhanced efficiency and accessibility. However, with the increasing digitisation of financial transactions, customer consent has become a true challenge. There are some regulatory methods and frameworks like GDPR, PSD2, CCPA, etc [19]. These methods in Europe have mandated customer data protection and management. Ontrust Solution is a fintech platform which has aimed to bridge the gaps between the compliance requirements and some seamless experiences.

B. Overview

The Ontrust solution is a fintech-driven consent management by the entire platform which has been designed to enhance customer trust and regulatory compliance. This enables some financial intuitions to obtain the chain of records and manage the whole customer consent while ensuring some industry regulations [19]. There are new solutions by which these digital banking and lending platforms allow the entire business to streamline the authorisation consent process to mitigate the risk and improve the experience of customers. With the help of AI-driven technology, blockchain on trust ensures transparency, reduced fraud, and enhanced accountability.

C. Problem Statement

Despite some new and advanced methods in fintech digital products, there are some problems which are related to customer consent management that persist. Many financial institutions have struggled to implement the whole transparent process [20]. There is some non-compliance with data protection regulations which leads to legal penalties, damage to reputations, and customer distrust. The traditional consent methods have often involved lengthy arguments, customer awareness, and engagement. So the lack of standardised technology will enhance some solutions to address.

doi: 10.48047/ijiee.2022.12.1.2

D. Objectives

The primary goals of this study are: 1. To have the effectiveness of Ontrust solutions in improving fintech customers' consent management and regulatory compliance. 2. To assess the impact of digital consent solutions on customer trust and experienced and financial decision-making. 3. To analyse the role of blockchain and AI in enhancing some new security and transparency in the fintech consent process. 4. To explore the whole industry's challenges and recommend some best practices for adopting digital consent solutions in financial institutions. The primary aim of the study is to examine how Ontrust solutions can enhance the whole customer consent management in FinTech while ensuring regulatory compliance, security, and user trust.

E. Scope and Significance

The entire scope of this study has focused on the role of Ontrust solutions in the fintech sector which has examined the impact on digital banking, payments, and lending platforms. This is significant for some financial institutions seeking compliance solutions and some policymakers who are aiming to strengthen data protection laws. So by addressing the key industry challenges this study contributes to improving the customer trust regulatory adherence and fintech innovations [20].

II. LITERATURE REVIEW

A. Regulatory frameworks and compliance in Fintech consent solutions

In these methods, the regulatory frameworks for the fintech solutions need to be designed to analyse and ensure data privacy, security, and some consumer rights protection for the digital financial ecosystem [1]. The General Data Protection Regulation (GDPR) in the European Union mandates that financial institutions have to be explicit and informed by the freely given consent of the users before processing their data.

This also provides the users the right to draw consent at any time. On the other side, the Revised Payment Service Directive (PSD2) in Europe has enforced strong customer authentication and mandates third-party service providers to analyse and access customer banking data with some clear user content. Similarly in the UK, the open bank regulations have required the adherence to strict consent management policies when charging the whole customer data with some third-party providers [2]. Thus, in the USA, the California Consumer Privacy Act gives the entire consumers greater control over personal financial data which has been required for the fintech companies to offer opt-in mechanisms and technology [3]. There is different compliance with these entire regulations which poses some challenges as the fintech firms must be balanced between the user experience and security and privacy requirements.

B. The role of blockchain and AI in digital consent solutions

Figure 1: Role of blockchain and AI [5]

doi: 10.48047/ijiee.2022.12.1.2

The addition of blockchain and artificial intelligence in digital consent solutions has significantly enhanced the security, transparency, and automation in Fintech. Blockchain technology provides some crucial tools of tamper-proof ledger, immutable which every instance of user consent, and this shave ensures the financial institutions cannot alter or misuse the customer approvals [4]. So this creates a verifiable and auditable trail for the consent transactions to reduce the risk of legal disputes.

Some effective methods of AI-driven authentication have played a crucial role in improving the entire security in coincident management [5]. AI enables some biometric authentication, behavioural analysis, and real-time fraud detection which makes sure that only authorised users grant consent. Artificial intelligence also enhanced the user experience by automating consent management and reducing some manual processes that provide consent options based on experience.

Thus, the entire Ontrust solution enables and leverages the blockchain to analyse and record the consent agreements and AI methods to authenticate whole users who are identified through facial recognition and fingerprint verification [6]. These important technologies not only give strength to security but also enhance compliance and trust ensuring that financial data-sharing methods are done ethically and transparently.

C. Customer trust and experience of the user in the Fintech consent process

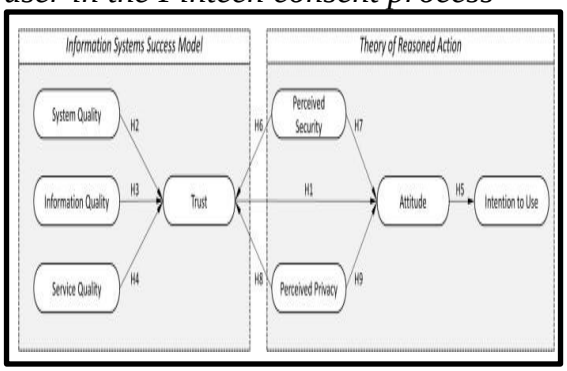

Figure 2: Trust-based Fintech adoption [7]

In fintech, customer trust is key and the design of a good digital consent has a direct impact on user confidence in financial services. For building trust, and understanding how the data of many users (personal data) is being kept as economic data, transparency around consent management is crucial [7]. A plain, simple, intelligible consent process ensures a good user experience that makes it easy for customers to see what data is collected, why, and on what basis it will be used. An example of this is Ontrust Solution which offers an easy-to-use interface to users for them to view, update, or withdraw their consent to their data at any given time. Consent agreements also impact customer engagement and retention to make the companies' marketing goals transparent [8].

There are fintech companies that allow customers with easy terms that are easy to understand and let people control their consent settings very simply, then customers will be more likely to use and recommend digital financial services. On the other hand, confusing and ambiguous consent policies can cause customer distrust, low engagement, and fines from the authorities [9]. With the user-friendly implementation of a secure consent solution, fintech companies improve the

doi: 10.48047/ijiee.2022.12.1.2

customer experience, fulfil compliance, and build long-term trust on the platforms.

D. Challenges and best practices in implementing digital consent solutions

There are many advantages to digital consent solutions for fintech firms but on the other side, there are several challenges in implementation, security, and compliance methods.

One of the major concerns is the complexity of regulatory requirements which differ across regions and require continuous updates to ensure compliance [10]. Some financial institutions have struggled with integrating consent solutions in which their whole existing systems have been analysed without disputing user experience. Some of the other challenges are cybersecurity threats, in which hackers target the fintech platforms to manipulate or steal the customary important data. So to protect the mechanism fraud-proof is very critical in preventing some unauthorised transactions and identity [11].

There are some additional fintech firms by which the customer education and many new users who do not fully understand the implications of the digital content may unknowingly approve the risky transaction. So to overcome these challenges fintech companies should adopt best practices methods like using blockchain for consent recording to ensure transparency and security. They have analysed leveraging is driven synthetically to verify the users and frauds [12]. Implementing some dynamic consent dashboards which have allowed users to manage approvals easily.

III. METHODOLOGY

A. Research Design

The entire study follows the explanatory research design, which helps to focus on understanding the impact of Ontrust solutions in fintech digital consent management. This investigates how regulatory compliance, AI, blockchain, and trust influence the consent process. This research explores the relationship between consumer behaviour, and fintech adoption, which provides insights into improving consent solutions.

B. Data Collection

This research depends on both qualitative and quantitative secondary data collection methods. Academic journals, articles, and books refer to the qualitative methods, and charts, graphs, and statistical data have also been shown in this research which highlights quantitative data methods.

C. Case Studies/Examples

Case Study 1: Enhancing digital consent with AI compliance

The company MasterCard has integrated some artificial intelligence across the network to analyse the security and compliance in digital transactions. Approx 143 billion transactions are done annually by the customers of Mastercard [13]. Mastercard AI-driven policies have significantly improved fraud detection and increased customer satisfaction rates.

Case Study 2: Blockchain for Secure Consumer Customer Management

JP Morgan Chase is at the forefront of adopting blockchain technology to enhance the security and transparency of customer segments. They have 3 trillion in profits in the markets and developed an immutable ledger for storing user consent agreements [14].

Case Study 3: Centric consent solution for open banking

Company Revolut has developed dynamic consent dashboards which have allowed the customers to manage financial data seamlessly. These initiatives have opened banking regulations, which provide users transparency and control over third-party access. This approach has been very important and boosted for the company [15].

doi: 10.48047/ijiee.2022.12.1.2

D. Evaluation Metrics

Evaluation metrics such as security, and compliance for fintech digital consent solutions, these being Ontrust, help to evaluate. This is about the compliance rate with regulations like GDPR, PSD2, and Open Banking to be compliant. Security improvements in the securities mechanism are evaluated in terms of fraud reduction, that is, the reduction of unauthorised transactions.

Consent revocation time (seconds) measures how quickly users can revoke permissions on the consent platform, while user adoption rate measures customer engagement with the consent platform [20]. Based on the feedback, the customer trust score (1-10) is the level of confidence in data protection. The last element is that system uptime (percent) guarantees uninterrupted consent management services. Moreover, these metrics reflect what is going well and not on the platform as well as how effective the regulators have been at monitoring transactions.

IV. RESULTS

A. Data Presentation

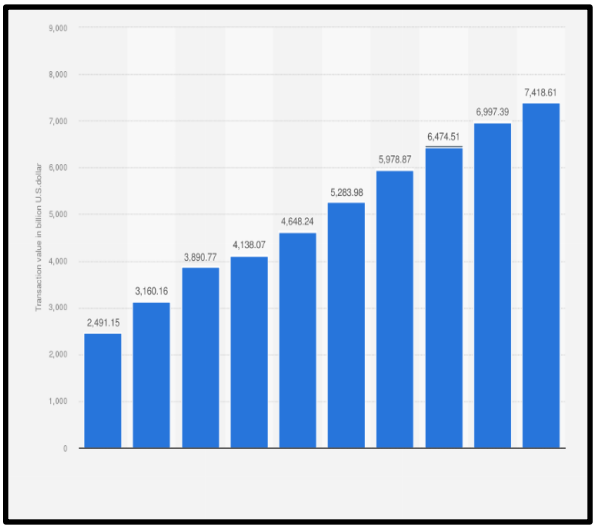

Figure 3: Trust-based Fintech adoption [16]

Transaction value augmented from $2,491.15 billion to $7,418.61 billion as progress was made in trust-based fintech adoption [16]. Growth increases consumer confidence and the realisation of fintech services between markets.

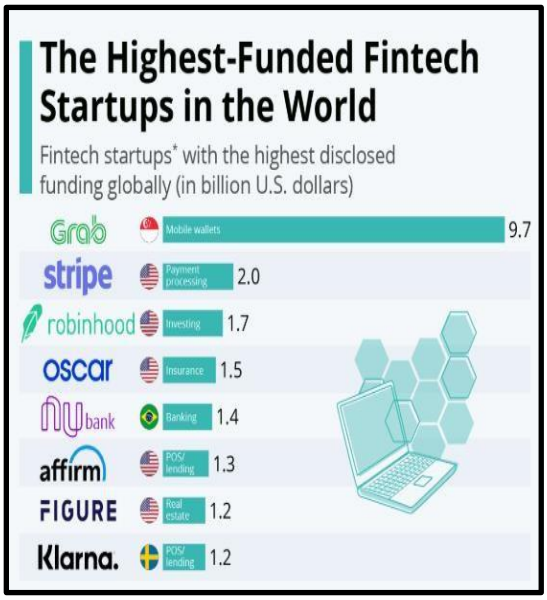

Figure 4: Trust-based Fintech adoption [17]

The graph depicts the major 'fintech' startups that have been funded at the highest levels in the world. This has a mobile wallet platform with $9.7 billion GRAB leads and then follows with $2.0 billion from payment processing by Stripe [17]. Oscar, NuBank, and Robinhood garnered $1.7 billion, $1.5 billion, and $1.4 billion, respectively, with funding concentrated within the various sectors [17].

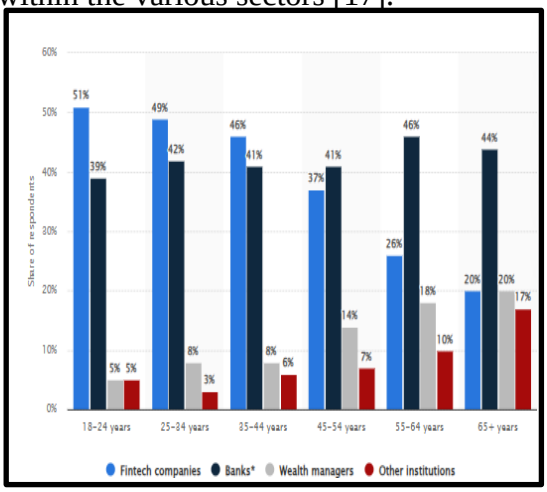

Figure 5: Trust-based Fintech adoption [18]

doi: 10.48047/ijiee.2022.12.1.2

In this graph, the breakdown of the trust in fintech brands compared to other financial service providers by age is presented. Younger demographics (18–24) best trust fintech companies (51%) while banks command the largest following among older demographics (65+; 44%) percent [18]. All age brackets have minimal trust in wealth managers and other institutions.

B. Findings

The findings highlight solution of Ontrust enhances consent management of customers within fintech by efficiently leveraging blockchain for securing, records and also AI for fraud detection significantly. The graphs illustrate the fast adoption of fintech on account of customer's trust in them and fintech innovation in their digital products. The fintech transactions that were trusted increased from $2.49 trillion to $7.42 trillion, which shows increased confidence [16].

Diverse fintech solutions are also well invested by leading startups such as Grab ($9.7 funding), Stripe ($2.0), etc [17]. Between demographics, trust is different banks (58% for over 55) for older groups and fintech (51% for 18–24) for younger ones [18]. There is a parallel between Ontrust's solution and digital products to help build tailored trust with service and customers with a different need at different ages. Therefore, the findings effectively emphasise the role of Ontrust in improving transparency, security, and regulatory compliance fostering trust within financial services digitally.

C. Case study outcomes

Case study	***Company***	***Key outcomes***
Enhancing Digital Consent with AI	**MasterCard**	This improved fraud detection by 20% which has increased customer satisfaction and regulatory compliance [13].
Blockchain to secure customer consent management	**JP Morgan Chase**	Developed an immutable ledger for consent storage which supported transparency with compliance with regulations [14].
Centric consent solution for opening banking	**Revolut**	Streamline data-sharing methods to improve user control over third-party access [15].

Table 1: Outcomes of the case study
(Source: Self-Created)

This table highlights the AI-enhanced detection of fraud detection, and blockchain-driven content storage and shows the company names and their effective outcomes.

D. Comparative Analysis

Authors	**Focus Area**	**Key Findings**	**Gaps**

doi: 10.48047/ijiee.2022.12.1.2

[1]	Regulatory framework for some fintech consent solutions	GDPR mandates some consent data processing, PSD2 enforces strong authentication	Global regulatory compliance challenges [1]
[2]	UK open regulations for banking	This requires strict adherence to analyse consent management for data sharing	Difficulty in balancing user experience methods
[3]	US regulatory compliance (CCPA)	Give consumers greater control over financial data	Challenges due to varying laws [3]
[4]	Blockchain in fintech consent solutions	Provides really tamper-proof, immutable ledger for financial transaction	Adoption barriers for fintech firms due to integration
[5]	AI-driven authentication in Fintech	Enhanced security via biometric authentication and fraud detection	Ethical concerns regarding AI and user data usage.
[6]	Ontrust solution AI and blockchain approach	Leverages blockchain consent for tracking and AI for biometric authentication [6]	Effectiveness in large-scale fintech environments
[7]	Trust of the customer and fintech adoption	Transparency in consent management boosts trust and improves engagement	Lack of standardisation in consent interface design
[8]	Impact of Consent Agreements on Customer Retention	A simple, clear process to increase the brand trust	Some policies can cause customer distrust
[9]	Regulatory	Confusing consent	Lack of enforcem

doi: 10.48047/ijiee.2022.12.1.2

	compliance and user experience challenges	policies leads to a fine	ent mechanism to ensure compliance
[10]	Challenges in regulatory compliance	Regulatory differences across regions create compliance burdens	Need for automated compliance solutions [10]
[11]	Cybersecurity threats in digital consent solutions	Hackers target fintech platforms more than often	Insufficient fraud detection methods for evolving threats
[12]	Best practice for fintech consent solutions	Blockchain ensures transparency [12]	Need for real-time compliance management systems.

Table 2: Comparative analysis

(Source: Self-Created)

The above table summarises some fintech consent solution studies and outlines the regulatory challenges (GDPR, PSD2, CCPA), the role of blockchain in some transparency, AI for some security, the need for standardised interfaces, automated compliance, and real-time management. Unlike most assertions in this area, this paper identifies gaps to increase the understanding of such integration barriers, ethical concerns, and cybersecurity threats.

V. DISCUSSION

A. Interpretation of Results

The growing trust in fintech digital products is brought to light due to the securing and transparent consent management of such products as Ontrust. Fintech continues to surge, attracting $2.49 trillion to $7.42 trillion worth of transactions through fintech as far as customer confidence is concerned particularly with the younger set of users opting for fintech over traditional banks [1]. Blockchain-based consent recording, AI-driven authentication, and easy-to-use dashboards bring out the additional level of this trust in Ontrust and all of this adds to the compliance and security [1]. Aligning with evolving customer expectations, Ontrust's dynamic consent management offer offers long-term customer engagement as well as regulatory adherence and promotes the automated use of fintech digital products across demographic groups.

B. Practical Implications

The adoption of fintech digital consent solutions such as Ontrust has a variety of implications on both the practical side of things for FinTech institutions and in particular for customers. It also ensures compliance with the changing compliance and regulatory norms like GDPR and PSD2 for companies, thereby saving them from legal and reputational risks.

Also, it increases the security protocols to evade fraud and identity theft. These solutions give customers more control and transparency when it comes to personal data meaning customers can rely on fintech platforms and have faith in them [3]. Further integration of AI and blockchain automates the processes even further with faster and more secure consent management. This enables operations with compliance to the standards.

doi: 10.48047/ijiee.2022.12.1.2

C. Challenges and Limitations

The implementation of digital consent solutions comes with some of the challenges. Integrating with legacy systems in financial institutions is susceptible and costly. Furthermore, customer education lags far behind its comparisons with other consenting online platforms, for the simple reason that many users are not cognisant of what it means to give consent in the digital world or even to read consent agreements [1]. Besides the issues of data privacy and cyber security risks, hackers are targeting consent management.

Also, interoperability between different platforms and regulatory environments is not easy, as fintech firms need to operate across the board in differing legal standards globally.

D. Recommendations

Fintech companies must initiate user education programs to educate their customers about the need for consent management and data privacy to overcome these challenges. In addition, integration with existing systems should be the priority, while using scalable and adaptable solutions, to cause as little disruption as possible. Multi-factor authentication and real-time fraud detection should be implemented as it is more secure [6]. Also, collaboration with regulators is needed to allow for the future-proofing of these consent solutions and compliance with the laws. Auditing and updating regularly will decrease emerging threats and increase trust.

VI. CONCLUSION AND FUTURE WORK

The incorporation of AI and blockchain for integration of fintech consent management allows Ontrust Solutions to significantly raise the bar on fintech about compliance, security, and trust of the users. The study shows that both user transparent, automated consent processes from regulatory adheres and build customer confidence. Although these challenges exist, there are, as yet, no solutions as of yet.

There are several future work directions to further improve the consent frameworks, increase interoperability amongst different platforms, and progress in developing methods for AI-driven fraud prevention. There is further research that would have focused on real-time compliance automation and user education initiatives to increase adoption. Consent management solutions will continue to be a primary area in which there will be continuous innovation for ensuring secure and trustworthy fintech systems.

VII. REFERENCE LIST

1. **Zyskind, G., Nathan, O., & Pentland, A.** (2015). "Decentralizing privacy: Using blockchain to protect personal data." *2015 IEEE Security and Privacy Workshops*, 180-184. https://doi.org/10.1109/SPW.2015.27
2. **Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K. K. R.** (2018). "Blockchain: A panacea for healthcare cloud-based data security and privacy?" *IEEE Cloud Computing*, 5(1), 31-37. https://doi.org/10.1109/MCC.2018.011791712
3. **Casino, F., Dasaklis, T. K., & Patsakis, C.** (2019). "A systematic literature review of blockchain-based applications: Current status, classification and open issues." *Telematics and Informatics*, 36, 55-81. https://doi.org/10.1016/j.tele.2018.11.006
4. **European Union Agency for Cybersecurity (ENISA).** (2019).

doi: 10.48047/ijiee.2022.12.1.2

"Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?" ENISA Report. https://www.enisa.europa.eu/publications/blockchain-and-the-gdpr

5. Chintale, P., Korada, L., Ranjan, P., Malviya, R. K., & Perumal, A. P. (2021). The Impact of Covid-19 on Cloud Service Demand and Pricing in the Fintech Industry. Journal of Harbin Engineering University, 42(7).
6. **Dai, H. N., Zheng, Z., & Zhang, Y.** (2019). "Blockchain for Internet of Things: A survey." *IEEE Internet of Things Journal*, 6(5), 8076-8094. https://doi.org/10.1109/JIOT.2019.2920987
7. **Marr, B.** (2018). "How blockchain will transform the supply chain and logistics industry." *Forbes*. https://www.forbes.com/sites/bernardmarr/2018/03/23/how-blockchain-will-transform-the-supply-chain-and-logistics-industry/
8. **Finck, M.** (2019). "Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?" *European Journal of Risk Regulation*, 10(2), 321-339. https://doi.org/10.1017/err.2019.48
9. **Zhao, J. L., Fan, S., & Yan, J.** (2016). "Overview of business innovations and research opportunities in blockchain and introduction to the special issue." *Financial Innovation*, 2(1), 28. https://doi.org/10.1186/s40854-016-0049-2
10. **Kou, G., Akdeniz, Ö. Ö., Dinçer, H., & Yüksel, S.** (2021). "Fintech investments in European banks: A hybrid IT2 fuzzy multidimensional decision-making approach." *Financial Innovation*, 7(1), 1-28. https://doi.org/10.1186/s40854-021-00239-0
11. **Chen, Y.** (2018). "Blockchain tokens and the potential democratization of entrepreneurship and innovation." *Business Horizons*, 61(4), 567-575. https://doi.org/10.1016/j.bushor.2018.03.006
12. Chintale, P. (2020). Designing a secure self-onboarding system for internet customers using Google cloud SaaS framework. IJAR, 6(5), 482-487.
13. **Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q.** (2020). "A survey on the security of blockchain systems." *Future Generation Computer Systems*, 107, 841-853. https://doi.org/10.1016/j.future.2017.08.020
14. **Gai, K., Qiu, M., & Sun, X.** (2018). "A survey on FinTech." *Journal of Network and Computer Applications*, 103, 262-273. https://doi.org/10.1016/j.jnca.2017.10.011
15. Chintale P: Optimizing data governance and privacy in Fintech: leveraging Microsoft Azure hybrid cloud solutions. Int J Innov Eng Res. 2022, 11:
16. **Kakavand, H., Kost De Sevres, N., & Chilton, B.** (2017). "The blockchain revolution: An analysis of regulation and technology related to distributed ledger technologies." *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2849251
17. **Lacity, M. C.** (2018). "Addressing key challenges to making enterprise blockchain applications

doi: 10.48047/ijiee.2022.12.1.2

a reality." *MIS Quarterly Executive*, 17(3), 201-222. https://aisel.aisnet.org/misqe/vol17/iss3/3/

18. **Marr, B.** (2019). "How much data do we create every day? The mind-blowing stats everyone should read." *Forbes*. https://www.forbes.com/sites/bernardmarr/2019/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/

doi: 10.48047/ijiee.2022.12.1.2