Are Digital Signatures in Blockchain Functionally Equivalent to Handwritten Signatures?

Victor Dostov[1,2], Svetlana Krivoruchko[1], Pavel Shust[3(✉)], and Victor Titov[2]

[1] Department of Financial Markets and Banks, Financial University Under the Government of the Russian Federation, 49 Leningradsky Prospekt, Moscow 125993, Russia
[2] Modern Financial Technology Laboratory of St Petersburg University, Saint Petersburg State University, 199034 St. Petersburg, Russia
[3] Russian Electronic Money and Remittance Association, Novoslobodskaya ul., 20, of. 25/A5ϕ, Moscow 127030, Russia
paul.shoust@gmail.com

Abstract. Digital signatures have different uses in a digital world, providing both identification of users and ensuring legal enforceability of digitally signed documents, making them legally binding for the signatories. Purpose of this paper is to review legal aspects of electronic signature application in modern technologies such as on-line banking, DLT and digital lending. As the latter are already well-researched, we use the case of online lending as an illustrative example, yet all conclusions and findings are equally valid for digitally signed transactions and blocks in DLT, for transactions in on-line banking and for many other cases. We look at the challenges presented by the remote conclusion of loan contracts and whether they can be addressed by the usage of electronic signatures. The focus of the research is whether there are technological of procedural solutions that can be used to ensure functional equivalence of electronic and handwritten signatures. The findings may provide grounds for further research of DLT application in electronic signature sphere.

Keywords: Consumer Loan Agreement · Electronic Signature Regulation · Handwritten Signature · Simple Electronic Signature · Distributed Ledgers

1 Introduction

Growing body of the academic literature suggests that distributed ledger technologies might be used to improve the efficiency and security of electronic signatures [1]. Moreover, distributed ledgers rely on electronic signatures to ensure identification, transparency, inalterability [2].

As there are no trust services providers in the blockchain, the trust is based on the e-signature keys and distributed inalterable ledgers. From practical standpoint, this means that private e-signature keys shall be reliably used in multitude of transactions, such as payments, transfer of value, authentication of legal documents, etc. In this regard, as

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2023
O. Gervasi et al. (Eds.): ICCSA 2023 Workshops, LNCS 14104, pp. 527–537, 2023.
https://doi.org/10.1007/978-3-031-37105-9_35

blockchain is based on electronic signatures, for legal interpretation of records in DLT there should be an assurance that e-signatures in general are functionally equivalent to handwritten signatures which are still a standard business practice worldwide. This functional equivalence is specifically important for distributed ledgers in particular, as there is no fallback option for handwritten signature.

There is somewhat patchy coverage of signatures (both electronic and handwritten) in academic literature. Legal concept of handwritten signatures is well discussed in in-depth analysis by Stephen Mason [3, pp. 1–94] covering both legal and historical aspects of the phenomenon. Lon L. Fuller [4] contributed significantly to understanding of a handwritten signature in an often-cited work on the functions of legal formalities. Applied aspects in mobile-based e-signatures [5], using electronic watermarks [6] are good examples of such technology-focused research. Another body of research is dedicated to electronic contracts which are intrinsically related to signatures, as well as act of 'signing' and mostly cover consumer protection issues: for example, material clauses disclosure [7], usage of standard electronic contracts and contracts on consuming digital content. But despite seemingly wide coverage of electronic signatures in academic literature, there are still gaps in understanding of relationship between electronic and handwritten signature as well as relation between electronic signature and electronic contract. This paper aims at starting to fill this gap by proposing methodological approach to analyzing practical implications of e-signature usage. From the methodological perspective, Veerpalu's [8] research provides the valuable perspective on functional equivalence regulation for the innovative processes and services.

Methodology of the paper is based on the comparative analysis of the existing handwritten and electronic signature regulation and synthesis of the outcome-focused approaches to achieving similar results in similar circumstances.

In this paper we describe the case of electronic contracts between borrower and lender in online lending services and identify the procedures that may strengthen reliability of online interaction between these two parties. The areas for further research are discussed as well.

2 Signature and Its Functions

In order to explore the potential role of DLT in the application of electronic signatures, it is necessary to first examine the various academic perspectives on the functions of signatures in general. Although electronic signatures are becoming increasingly prevalent, most of the existing academic literature still focuses on handwritten signatures, which remain more widely used. It is also notable that legal considerations are a primary focus of this analysis, rather than technological elements of signatures. However, we contend that an overview of this discussion remains relevant, as the functional equivalence of handwritten and electronic signatures (whether DLT-based or not) must be established within the existing legal framework in order for electronic signatures to gain widespread acceptance among individuals and businesses. It is interesting to note that there is no universally accepted definition of a signature in academic literature. For instance, the United States Commercial Code defines a signature as "any symbol executed or adopted by a party with present intention to authenticate a writing" [9, p. 1185]. A more high-level definition is proposed by the Oxford Dictionary: 'a sign or a mark impressed upon

anything'. From the general perspective the signatures are considered a 'legal formality' [4, pp. 800–801].

The definitions of signatures provided by existing academic literature are notably technology and instrument-neutral, which may seem counter-intuitive for subsequent discussions about electronic signatures. However, this approach is justified from a legal standpoint, as it ensures that business practices and courts recognize the varying circumstances and environments in which parties interact. Put simply, a signature may be a sophisticated instrument or a simple mark, made on a piece of paper or a napkin, for a multitude of reasons. This is a critical consideration for understanding the factors that contribute to the success of electronic signatures. While much of the discourse surrounding electronic signatures focuses on the instruments themselves (such as token or cloud-based signatures, or SIM-card-based solutions), or on the storage of qualified electronic signatures, it is important to recognize that the true universality of electronic signatures (including those issued on DLT) will depend on their ability to be used in a wide range of circumstances. Additionally, there is a significant body of literature exploring the various functions that signatures serve.

The approach to handwritten signatures is technology-neutral, making it irrelevant to categorize them based on the instrument or material used. Formally speaking, it is possible to make categorizations based on the type of instrument used to put a handwritten signature (e.g. pen or pencil) or the material on which the handwritten signature is placed (e.g. paper, wood or something else). But the function of the handwritten signature remains the same regardless of these theoretical categories. However, electronic signatures are very technology-specific, which makes them inherently different from handwritten signatures. It is important to consider that by introducing new technologies to the signatures realm, we are not only improving the efficiency of the process but also changing centuries-long business traditions.

There are three types of electronic signatures with varying assurance levels: simple electronic signature (SES), advanced electronic signature (AES), and qualified electronic signature (QES). Simple electronic signatures provide the lowest level of assurance since they do not verify the identity of the signatory and are only associated with electronic data. "I agree" buttons and tickboxes on websites are examples of simple electronic signatures. Even the signature in an email might be recognized as a simple electronic signature. The downside of simple electronic signatures is that their enforceability usually requires a court decision.

Advanced electronic signatures [10] are generally more reliable, as they allow to identify any subsequent changes to the signed documents. Advanced electronic signatures are also uniquely linked to the signatory, specific procedures are used to ensure that the signature cannot be used by anyone, except the signature holder.

Qualified electronic signature is essential and advanced electronic signature that is issued by the reliable third party (qualified trust service provider) which allows to undoubtedly identify the signatory (see Table 1).

Anecdotal evidence and experience shows that there is an inverse relationship between the level of assurance provided by electronic signatures and their adoption rates. This means that people are more willing to use simpler electronic signatures even

though they provide less legal protection. This is an important consideration for developers, as technology can provide the highest level of assurance and inalterability, but a higher entry level can negatively affect adoption. Users tend to prioritize convenience over risks unless one of them is critical. Therefore, developers need to balance the level of assurance with the ease of use to ensure wider adoption of electronic signatures.

Table 1. Functional comparison of SES, AES, and QES.[1]

	Simple electronic signature	Advanced electronic signature	Qualified Electronic Signature
Identification function	-	+	+ (highest assurance level as QES is issued by the third party universally trusted by all actors)
Expression of intent	+	+	+
Inalterability function	-	+	+
Evidential function	+	+	+

As previously discussed, signatures must serve specific functions to be of value to economic actors. In the following section, we will examine the evidentiary, cautionary, and inalterability functions of signatures, as well as their ability to record the expression of intent. Additionally, we will explore the risks associated with using signatures and methods for mitigating those risks.

In terms of its evidentiary function, a signature serves to confirm the existence of a legally-binding document, leaving a physical or electronic artifact as evidence. The viability of this artifact is crucial in order to prove the existence of the contract. From the perspective of DLT, viability is based on the distributed nature of information storage and the built-in inability of any single actor to unilaterally delete information. The architecture of DLT must account for the need to maintain evidence over a long period of time, particularly in cases where permissionless DLT relies on the unofficial agreement of its participants. A viable electronic signature based on DLT must ensure that actors cannot simply decide to stop supporting it, which would effectively result in a loss of access to information. However, permissioned DLT systems may be subject to other risks, such as the potential for the central operator to manipulate data in the absence of proper technological safeguards. In such cases, it may be necessary to establish legal obligations to ensure the independence and stability of the system, similar to the specific requirements imposed on qualified trust service providers by relevant regulations.

The cautionary function of a signature requires that it be a significant act for the signatory, signifying their entry into the contract. This is particularly important for contracts that involve new responsibilities and liabilities, such as in the case of lending, which will be discussed in detail below. The importance of the cautionary function

[1] Adapted from [11].

may vary significantly depending on cultural circumstances and tradition [12]. From the perspective of electronic signatures, the cautionary function may not be as critical, but the process of using an electronic signature should still entail certain formalities or procedures, rather than being fully automated. While this may seem counter-intuitive from a technical perspective, it is an important consideration in the context of business interactions.

The record-keeping function of a signature is self-explanatory and is similar to the evidentiary function. Handwritten signatures are typically placed on durable material such as paper, but electronic signatures require specific rules and procedures to ensure that they are recorded in an unalterable manner and can be accessed over time. It is also important to ensure reverse compatibility, allowing actors to verify electronic signatures even after the technology has become outdated and is no longer actively supported.

The purpose of signatures is to ensure that the document cannot be altered. However, traditional methods of signing multi-page documents, such as signing every page, are not very reliable. Qualified electronic signatures are a much better option as they allow any changes to be identified. Additionally, DLT can provide an extra layer of reliability as the document or its hash can be stored on a distributed ledger.

There is ongoing debate among practitioners on whether DLT can accommodate legitimate changes to contracts. While some believe that contracts should be fixed, real business practices often require changes to be made to certain clauses. It is possible to simply sign a new version of the document and store it on the distributed ledger as a new version of the existing document. However, it is important to consider whether DLT can handle the growing volume of data.

Another function of the signature is the expression of intent. However, this function does not depend on technological solutions and is largely self-explanatory. Rather, the expression of intent is ensured through the rules and procedures governing the use of electronic signatures.

The functions of a signature discussed above are by no means exhaustive, and different research perspectives may emphasize different types of functions. Nevertheless, the outlined functions have allowed us to identify potential risks associated with the use of signatures, whether handwritten or electronic. This analysis highlights potential gaps in the long-standing tradition of handwritten signatures and provides insight into how DLT considerations can be integrated into electronic signature practices.

The identification of signatories through the use of signatures is limited in its effectiveness. This is because handwritten signatures are not bound to any particular form or technology, unlike identity documents that are commonly used for verification purposes. Consequently, this exposes signatures to the risk of forgery, which can result in identity fraud, significant financial losses, and legal disputes. Furthermore, the occurrence of forgery undermines trust in the economy and the technology used to facilitate electronic signatures.

The implementation of Distributed Ledger Technology (DLT), such as blockchain, in electronic signatures does not wholly address the risk of identity fraud. Permissionless DLT networks, like Bitcoin, lack complete personalization and do not guarantee reliable identification of users. Although software can assist in identifying the identities behind Bitcoin wallets, the possibility of error remains. Moreover, the reliability of identification

hinges on the involvement of specific actors in the transaction, which renders DLT-based electronic signatures unreliable for day-to-day use, particularly in lending.

To mitigate the risk of identity fraud, specific identification procedures must be established. Fortunately, such procedures are well-established in the financial sector and other industries. The level of identity verification required should be proportionate to the level of assurance required for a given scenario. Overly strict identification requirements can negatively impact the usability of electronic signatures and give rise to data protection concerns. Therefore, it is essential to consider the specific requirements for various situations when developing DLT-based electronic signature solutions. For example, the level of identification required to purchase groceries differs from that needed to apply for a loan at a bank.

Despite the type of signature used, there is a risk of coercion that individuals may face when signing documents. They could be pressured or tricked into signing a document without fully understanding its contents. This could result from direct fraud or unclear wording in a legal contract [13, p. 731], whether intentional or unintentional. In addition, individuals may be coerced into entering into business relationships under peer pressure, for instance. The risk of coercion is relevant regardless of the type of signature used, including electronic signatures. However, the risks of coercion may be even higher with DLT technology due to the inalterability of records and information included in the ledger. This means that a falsely signed document will be kept on the distributed ledger indefinitely, which raises legal questions in case of disputes. To address this issue, procedures must be introduced to allow for the dispute of signatures if they are proven to have been applied under coercion or not in good faith. Failure to do so would limit the universal usage of DLT-based electronic signatures. Interestingly, the inalterability of DLT may be useful for investigative purposes, as it prevents actors from covering their tracks and hiding illicit activities ex-post. It is important to note that the risk of coercion is distinct from limited knowledge or literacy, as the fact that a document was signed in good faith does not guarantee that the signatory actually read and understood its contents [14]. This applies to both electronic and handwritten signatures.

3 Signatures in the Financial Market: Case of Lending

The case of lending in the financial market provides an excellent opportunity to showcase the multitude of functions that electronic signatures can perform. This is because trust is a major concern in the lending sector, where lenders are often skeptical of borrowers and want to ensure that they receive their money back in a timely manner. At the same time, borrowers are concerned that lenders may abuse their position and charge exorbitant fees and commissions. These issues are further compounded by the fact that lending in the financial market is associated with high legal risks. Potential conflicts between lenders and borrowers may need to be resolved in court, and it is crucial to have an appropriate document trail to protect the interests of both parties.

In addition, lending is a financial service that is subject to specific regulations, such as anti-money laundering regulations. This adds to the complexity of the lending process and underscores the importance of having a secure and reliable system for managing loan agreements and associated documentation. As such, the lending sector provides a

perfect illustrative example of a situation where lack of trust is exacerbated by legal risks and specific legal requirements.

By examining the functions of electronic and handwritten signatures in this context, we can also identify areas where distributed ledger technology can be used to improve efficiency, enhance security, and increase reliability.

Table 2. Expected outcomes of the signature function and their business purposes (case of lending).

Outcome	Business purpose
Identification of parties	Money laundering/terrorist financing risks mitigation Enforceable legal redress
Record of expression of intent	Efficient enforceability and protection against fraud, contesting the contracts
Inalterability	Protection against unilateral changes of contract
Contract as evidence	Possibility to enforce the contract through the legal system

Throughout the lending process, the parties use signatures and contracts to ensure the following outcomes (see Table 2):

- *Identification of the parties.*

The lending sector presents a unique case of reverse information asymmetry, where the lenders have limited access to information that is critical to making informed decisions. While it is true that customers may have limited access to information to compare offerings from different financial services providers, in the case of lending, lenders also face significant informational challenges.

Financial institutions must first verify the identity of potential borrowers to ensure that they are not involved in money laundering, terrorist financing, or belong to higher-risk groups, such as politically exposed persons. This is a requirement of specialized regulation, and failure to comply with these regulations can result in severe penalties.

Moreover, lending is data-driven, meaning that lenders need to collect and analyze information about potential borrowers to determine their creditworthiness. This involves evaluating factors such as credit history, income, and other financial indicators to assess the borrower's ability to repay the loan.

Customer due diligence is based on the level of assurance, as mentioned by Shust and Dostov [15]. This process requires the verification of identity, which cannot be accomplished solely through signatures. Handwritten signatures can act as a factor in verifying identity, but only after costly expertise. In contrast, qualified electronic signatures (QES) are efficient in this regard, as they are provided after identity verification, unlike handwritten signatures that can be used without any prerequisites.

It is crucial to ensure that QES certificates are not anonymous if the qualified certificates are issued and stored on the blockchain. However, it is important to note that there are multiple ways to verify identity apart from signatures, such as video identification or biometric identification [16].

Of course, electronic signatures cannot be used to assess creditworthiness of the potential borrower [17] and multitude of other methods are used instead [18]. Below we are looking at particular circumstances where electronic signatures perform these functions. This analysis will be based on the case of loan provision. However, the same consideration will apply in other cases and business scenarios as well.

– *Recording the expression of intent*

In the lending process, financial institutions must ensure that borrowers not only qualify for a loan but also willingly accept all associated terms and conditions. This is crucial not only for regulatory purposes, where financial institutions are mandated to explicitly state the terms and conditions of the contract, but also to prevent potential identity fraud claims. It is essential that the borrower's intent is expressed explicitly and that the evidence of their agreement is admissible in court.

When viewed as a process rather than an instrument, signatures (whether electronic or handwritten) are an efficient tool to express intent. However, they cannot ensure that the customer (potential borrower) has fully read and understood the contract, as the contract can be difficult to comprehend due to legal jargon [19]. Nevertheless, signatures can be used to fix that the borrower has actively agreed to the terms and conditions of the agreement.

To offset this risk, many financial regulators have established requirements towards the form and contents of contracts [20]. These requirements also help to avoid "Russian doll" contracts, which can create cascading complexity as certain clauses reference other contracts that link to additional references.

Electronic signatures are effective in fixing the expression of intent because they imply certain procedures that the customer must follow to ensure that their intent is properly recorded and collected. Even if certificates are stored on a distributed ledger, practitioners need to ensure that the process of using this signature appropriately captures the intent of the customer.

– *Inalterability*

Loan agreements in the lending sector typically contain critical information such as the lending rate, loan amount, and repayment schedule. It is crucial to ensure that these documents are not altered subsequently, as any changes can lead to disputes between the financial institution and the borrower. This is important for both parties, as each can dispute the terms of the agreement in court.

When using paper documents, ensuring inalterability is mostly a logistical issue. It's important to make sure the document is not destroyed or subsequently altered. The same issue is relevant for electronic documents, and in this regard, electronic signatures (namely, qualified electronic signatures) are much more efficient than handwritten signatures. The same is true for distributed ledger technology, which is praised for its inalterability, among other things.

In addition to preventing direct and explicit fraud, inalterability may also help with improper business practices. For example, research shows that unilateral changes to contracts might be against general e-commerce legal requirements [21].

However, ensuring inalterability in current business scenarios can be rather complicated. Financial institutions may be forced to support large document storage facilities,

develop specific practices for handling and managing these archives, and keep documents on record for 3–5 years depending on jurisdiction. For public electronic contracts, this requires publishing all versions on the financial institution's website, which is impractical and raises questions about what will happen in case of the closure of the financial service provider.

With distributed ledger technologies and qualified electronic signatures, the same result can be achieved with lower costs. However, to ensure the universal or at least wider implementation of this technology, financial institutions need to ensure that the technology is interoperable and does not create data silos. This is an important issue to consider in the communities' further efforts to expand the usage of DLT in electronic signatures.

– *Evidence*

It is essential to ensure that the documents signed between the lender and the borrower are admissible evidence in court and cannot be tampered with.

The reliability of electronic signatures as evidence in case of disputes depends on their ability to fulfill all necessary functions. The inalterability of distributed ledgers may contribute to ensuring the reliability of electronic signatures stored on them. However, legal recognition of such documents and signatures is also crucial. The legal framework should recognize documents and electronic signatures stored on distributed ledgers to ensure their admissibility in courts. This applies not only to single documents but also to the general audit trail of all documents and transactions in the retail and corporate banking sectors [22, p. 25]. The audit trails should allow the reconstruction of the flow of transactions [23] and underlying contractual documents, which can greatly aid in supervisory and law enforcement activities. As such, the combination of the technological and legal aspects is necessary to ensure the reliability of electronic signatures as evidence in case of disputes.

4 Conclusions and Further Research

Purpose of this paper is to highlight rather counterintuitive nature of signatures as legal formalities. Highest assurance levels do not warrant the universal adoption of electronic signatures, even though they can bring additional benefits to the economic actors.

This consideration shall be taken into account when discussing DLT infrastructure and usage of distributed ledgers in context of electronic signatures. DLT can bring meaningful positive impact on the reliability of electronic signatures and storage of digitally signed documents (i.e. to ensure their inalterability). On the other hand, it is critical to adapt these technological solutions to the business practices and a common sense. The inalterability function is a good illustration of this. Keeping documents in the state as they were initially signed is extremely important to protect against fraud. But this complicates situation in cases of coercion and fraud–victims may have difficulties with rectifying errors.

This makes it extremely important to complement ongoing efforts to improve the efficiency of distributed ledgers with analysis of the business practices, legal considerations, and review of the user experiences. Overlooking these aspects may make technological efforts futile, as they will not be widely adopted.

Electronic and handwritten signatures alone cannot fulfill all of the functions required by business practice. Additional procedures and processes, such as identity verification, must be employed to complement the usage of electronic signatures effectively.

However, despite this limitation, there are areas in which distributed ledger technology (DLT) can improve the usage of electronic signatures in various sectors, including finance. For example, leveraging the inalterability of documentation stored and signed on distributed ledgers can provide greater transparency and confidence in the validity of signatures. Additionally, the use of DLT can enhance the security of electronic signatures by providing an immutable record of transactions that can be audited if necessary.

One area of concern when implementing DLT-based electronic signature systems is the verification of user identity. Legal requirements for identity verification must be taken into consideration to ensure that any new technological proposition is compliant with regulations and ultimately contributes to the attainment of its goals. Ensuring compliance in this area can also help in achieving wider business adoption of DLT and its integration into various business processes.

Thus, while electronic and handwritten signatures may have limitations, the integration of DLT can enhance their functionality and reliability, improving the overall efficiency and effectiveness of business processes.

References

1. Krylov, G., Gaybatova, A., Davydenko, V., Grigoryan, A.: Integration of distributed ledger technology into software electronic signature exchange service. Procedia Comput. Sci. **169**, 479–488 (2020)
2. Sunyaev, A. Distributed ledger technology. In: Internet Computing, pp. 265–299. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-34957-8_9
3. Mason, S.: The Signature. Electronic Signatures in Law. University of London Press (2016)
4. Fuller, L.L.: Consideration and form. Columbia Law Rev. **41**(5), 799-824 (1941).https://doi.org/10.2307/j.ctv5137w8.7
5. Ruiz-Martínez, A., Sánchez-Martínez, D., Martínez-Montesinos, M., Gómez-Skarmeta, A.F.: A survey of electronic signature solutions in mobile devices. J. Theor. Appl. Electron. Commer. Res. **2**(3), 94–109 (2007)
6. Zhu, L., Zhu, L.: Electronic signature based on digital signature and digital watermarking. In: 5th International Congress on Image and Signal Processing, pp. 1644–1647. IEEE, Chongqing (2012). https://doi.org/10.1109/CISP.2012.6469828
7. Kaviar, H.: Consumer protection in electronic contracts. Int. Arab J. e-Technol. **2**(2), 96–104 (2011)
8. Veerpalu, A.: functional equivalence: an exploration through shortcomings to solutions. Baltic J. Law Polit. **12**(2), 134–162 (2019). https://doi.org/10.2478/bjlp-2019-0015
9. Hays, M. J.: The E-sign act of 2000: the Triumph of function over form in American contract law. Notre Dame L. Rev **76** (4,) 1183–1214 (2001)
10. Regulation (EU) No 910/2014 of the European Parliament and of the council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&from=EN#d1e2403-73-1. Accessed 21 Apr 2023

11. Titov, V., Shust, P., Dostov, et al.: Digital transformation of signatures: suggesting functional symmetry approach for loan agreements. Computation **10**, 106, 2022, https://doi.org/10.3390/computation10070106
12. Cary, P.: A brief history of the concept of free will: issues that are and are not germane to legal reasoning. Behav. Sci. Law **25**(2), 165–181 (2007). https://doi.org/10.1002/bsl.748
13. Becher, S.I.: Asymmetric information in consumer contracts: the challenge that is yet to be met. Am. Bus. Law J. 45(4), 723–774 (2008). https://ssrn.com/abstract=1016010. Accessed 20 Mar 2023
14. Stiglitz, J.E.: The contributions of the economics of information to twentieth century economics. Q. J. Econ. **115**(4), 1141–1478 (2000). https://doi.org/10.1162/003355300555015
15. Shust, P., Dostov, V.: Implementing innovative customer due diligence: proposal for universal model. J. Money Laundering Control **23**(4), 871–884 (2020). https://doi.org/10.1108/JMLC-01-2020-0007
16. FATF: Anti-money laundering and terrorist financing measures and financial inclusion - With a supplement on customer due diligence. FATF, Paris, pp. 1–117 (2013–2017). www.fatf-gafi.org/publications/financialinclusion/documents/financial-inclusion-cdd-2017.html. Accessed 21 Mar 2023
17. Hwang, B-H., Tellez, C.: The Proliferation of Digital Credit Deployments. CGAP Brief, World Bank, Washington, DC, pp. 1–4 (2016)
18. Berg, T., Burg, V., Gombović, A., Puri, M.: On the rise of FinTechs: credit scoring using digital footprints. Rev. Finan. Stud. **33**(7), 2845–2897 (2020). https://doi.org/10.1093/rfs/hhz099
19. Gindin, S.E.: Nobody reads your privacy policy or online contract? Lessons learned and questions Raised by the FTC's action against sears. Northwest. J. Technol. Intellect. Prop. **8**(1), 1–39 (2009)
20. Kunz, C., Del Duca, M., Thayer, H., Debrow, J.: Click-through agreements: strategies for avoiding disputes on validity of assent. Bus. Lawyer **57**(1), 401–429 (2001). https://doi.org/10.2307/40688063
21. Loos, M., Luzak, J.: Wanted: a bigger stick. on unfair terms in consumer contracts with online service providers. J. Consum. Policy **39**(1), 63–90 (2015). https://doi.org/10.1007/s10603-015-9303-7
22. English, J., Abdou, H., Adewunmi, P.: An investigation of risk management practices in electronic banking: the case of the UK banks. Banks Bank Syst. **9**(3), 1816–7403 (2014)
23. Westerlund, M., Neovius, M., Pulkkis, G.: Providing tamper-resistant audit trails with distributed ledger based solutions for forensics of IoT systems using cloud resources. Int. J. Adv. Secur. **11**(3,4), 288–300 (2018)