Transforming Credit
Guarantee Schemes with Distributed Ledger Technology

Sabrina Leo[1] , Andrea Delle Foglie[1] ,
Luca Barbaro[1] , Edoardo Marangone[1] , Ida Claudia Panetta[1] , and Claudio Di Ciccio[2]

[1] Sapienza University of Rome, Rome, Italy, `name.surname@uniroma1.it`
[2] Utrecht University, Utrecht, Netherlands, `c.diciccio@uu.nl`

Abstract. Credit Guarantee Schemes (CGSs) are crucial in mitigating SMEs' financial constraints. However, they are renownedly affected by critical shortcomings, such as a lack of financial sustainability and operational efficiency. Distributed Ledger Technologies (DLTs) have shown significant revolutionary influence in several sectors, including finance and banking, thanks to the full operational traceability they bring alongside verifiable computation. Nevertheless, the potential synergy between DLTs and CGSs has not been thoroughly investigated yet. This paper proposes a comprehensive framework to utilise DLTs, particularly blockchain technologies, in CGS processes to improve operational efficiency and effectiveness. To this end, we compare key architectural characteristics considering access level, governance structure, and consensus method, to examine their fit with CGS processes. We believe this study can guide policymakers and stakeholders, thereby stimulating further innovation in this promising field.

Keywords: Distributed Ledger Technologies · Blockchain · Credit Guarantee Schemes · SME Finance

1 Introduction

In the credit industry, a guarantee reduces the financial risk of loans by providing a lending bank with additional assurances, increasing the likelihood of capital.[3] It also signals the borrower's intention to repay, reducing monitoring costs. Credit Guarantee Schemes (CGSs) act as a third-party provider of credit risk mitigation to lenders. By effectively reducing the risk associated with lending, they incentivise financial institutions to extend credit to Small and Medium-sized Enterprises (SMEs), thereby enhancing their financial stability and prospects for growth. CGSs received increased attention during the COVID-19 pandemic as government credit guarantee programmes improved banks' balance sheets and facilitated credit extensions to creditworthy businesses. The positive impact on post-crisis productivity was attributed to expanded coverage and simplified procedures in these schemes [7,10].

However, the literature has highlighted the financial sustainability issues of CGSs, particularly the risk of high default rates, which can force them to pay significant rewards [2]. A common criticism concerns the lack of transparency between the parties involved in the transaction (from customer to CGS and from bank to CGS), which leads to problems such as

---

[3] European Central Bank: "What is collateral?" (2016): `www.ecb.europa.eu/ecb/educational/explainers/tell-me/html/collateral.en.html`

moral hazard for borrowers or adverse lender selection. Furthermore, the correct assessment of the customer's creditworthiness and the procedure's cost-effectiveness influence the credit guarantees' additional attributes. Therefore, CGS's potential also depends on the sustainability and efficiency of its operational processes.

Emerging Distributed Ledger Technologies (DLTs), such as blockchain, open up a chance for processes involving third parties to be trustworthily executed [13], particularly in scenarios where there is a lack of mutual trust and confidence between the parties. Specifically, by leveraging blockchain's main features, including operational traceability and transparency, it is possible to minimise the risk of fraudulent activities, enhance customer trust, lower operational costs through process automation support, and reduce downtime.

In this paper, we describe the main challenges and opportunities of blockchain technology adoption for addressing the inherent weaknesses of traditional CGSs. We also suggest a complete framework that includes all the important steps in the CGS operational process, from the application to possibly enforcing safety measures. This framework will help identify key areas that could benefit from integration with DLTs. Given the specificity of the procedures, the actors involved, and data sensitivity in transactions, our paper raises questions about the appropriate blockchain architecture that can improve transparency, security, and automation throughout the entire CGS lifecycle. Our paper provides a roadmap for policymakers, financial institutions, and stakeholders who seek to modernise and optimise CGS mechanisms. To the best of our knowledge, this is the first endeavour exploring a synergy between DLT and CGS. We hope it can serve to stimulate further research and innovation in this nascent yet promising field.

In the following, Sect. 2, outlines the core ideas that form the basis of our proposal. In Sect. 3, we discuss why given blockchain configurations are suitable our setting. Section 4 describes their possible application in the credit guarantee life cycle. Finally, Sect. 5 concludes the paper.

2 Background

2.1 Distributed Ledger Technologies

Distributed Ledger Technologies (DLTs) comprehend protocols designed to enable the transactions' storage, processing, and validation within a decentralised network of interconnected peers. A distributed ledger is a registry replicated over a network of computing systems (henceforth, *nodes*) that records the sequence of transactions containing the transfer of value or data between sender and recipient accounts [11]. Its distributed architecture obviates the necessity for centralised authorities or intermediaries in data management. Every transaction within this framework features a timestamp and a unique cryptographic signature to prove that the account's owner issued it. Signatures are generated utilising a public/private key scheme, where each user possesses an account associated with a distinct address to which these keys are linked. This setting guarantees pseudonymity. We recall that pseudonymity differs from anonymity in that a unique identifier (in this case, the account number) is associated with the same individual, singled out across the registered data. The list of the shared transactions contained in the ledger is accessible to all network participants (owing to its public nature) so that everyone can verify that the digital signature belongs to the owner and trace all the transfers from or to an account.

Blockchain, a widely known class of DLT, entails aggregating of ledger segments into blocks, which are then sequentially linked backwards to form an immutable chain. The integrity

of DLTs, including blockchain, is fortified through a confluence of cryptographic methodologies and the distributed validation of transactions. In blockchains, every block is linked to the preceding one by keeping in the former a fingerprint number identifying the latter. This fingerprint is yielded by a mathematical function called *hashing*. Hashing produces a number (the hash). It is deterministic (given the same data, the same hash is returned) but one-way (hashes cannot be reverse-engineered to retrieve the input). Altering a bit turns the associated hash into a completely different number. Well-known blockchain platforms such as Bitcoin [22], Ethereum [27], and Algorand [5] necessitate transaction fees to allow for the submission and processing of transactions. Fees serve as an economic incentive to remunerate the computing systems in the network which include and maintain the infrastructure up and running. To ensure a single, reliable and generally acknowledged version of the transaction record, blockchains rely on consensus algorithms. These algorithms guarantee that all participants agree on the content of the ledger and that only trusted nodes can add new information. Proof of Work (PoW) [15] and Proof of Stake (PoS) [24] are two renowned consensus mechanisms used to validate transactions and add new blocks to a blockchain. Blockchain platforms such as Ethereum and Algorand offer the capability to execute **smart contracts**, namely executable programs that are deployed, stored, and run within the blockchain environment [8]. Smart contracts' operations are triggered by transactions, hence without the involvement of a trusted third party. Therefore, the history of invocations can be verified, replayed and trusted throughout the whole network. As with transactions, the execution of smart contract code is subject to costs that fall under the name of *gas* in the Ethereum nomenclature. These costs depend on the complexity of the invoked code and the amount of data exchanged and stored. To reduce the invocation costs of smart contracts, external peer-to-peer systems are typically employed to save larger chunks of data. **Inter Planetary File System (IPFS)**[4] is one of the most commonly used distributed systems to store data across multiple peers without the involvement of any central authority or trusted organisation. The address of an IPFS file is based on the hash of the file itself, so that the contents and its locator are immutably bound. The locator is thus typically saved by smart contracts, which permanently store the link to that resource on-chain.

Blockchains are often classified according to transactability (public or private) and consensus mechanism (permissionless or permissioned). If a blockchain is **public**, every node is endowed with the capability to initiate and monitor transactions. This fosters a transparent environment readily accessible to any users. In contrast, the blockchain is **private** if only selected nodes are entitled to participate in transaction initiation and observation. If any node in the network can participate in the consensus decision-making process, the blockchain platform is **permissionless**. Instead, if only specific nodes can determine the next status of the blockchain, it is **permissioned**. As a result, blockchain platforms are typically classified into four different categories: public permissionless, public permissioned, private permissionless and private permissioned. These characteristics discriminate the suitability of a blockchain platform to a given application scenario.

2.2 Credit Guarantee Schemes

SME credit markets are known for experiencing financial constraints and imperfections such as information asymmetries, insufficient or absence of recognised collateral, high transaction

---

[4]`ipfs.tech`

costs for small-scale lending, and perceived high risk, all contributing to suboptimal credit allocation. In this scenario, CGSs are crucial in offering lenders third-party credit risk mitigation to enhance SMEs' credit availability, acting as a strategic component in the market for credit distribution, and minimising distortions in credit markets. Moreover, CGS can operate as a tool at the disposal of policymakers to help SMEs finance during an economic downturn when risk aversion rises and a credit crunch is expected [28].

Numerous stakeholders partake and engage in the proceedings. **Government agencies** or Ministries oversee public CGSs by providing policy guidance, funding, and regulatory frameworks. From their standpoint, CGSs are an integral part of national development strategies, promoting the growth of SMEs and financial inclusion [25]. **Credit Guarantee Institutions (CGIs)** manage CGSs, evaluate credit risk, provide guarantees, and handle claims. They work with lenders to reduce credit risk and promote financing for SMEs [18]. **Credit institutions** such as banks and microfinance institutions work with CGSs and CGIs to provide lower-risk loans to SMEs. The ultimate beneficiaries of CGS-guaranteed credit are **SMEs** (generally speaking, the borrowers), who use it to finance their operations and promote investment, growth, and job creation. CGS enhances credit rating to facilitate business expansion. **Investors and shareholders**, according to the type of funds provided (i.e., Mutual Guarantee Institutions [14], Corporate Guarantee Schemes, Public Guarantee Schemes), expect different types of returns when supporting the development of SMEs. **External auditors** independently evaluate the financial status and adherence to CGI regulations by assessing their efficiency in supporting the funding of SMEs. One of the multiple challenges associated with evaluating a CGS concerns providing useful information for the decision-making of agents who maintain an interest in the entity [17]. Not all stakeholders have a similar degree of information at their disposal. On the one hand, internal stakeholders, such as managers, have unlimited access to information. On the other hand, external stakeholders, such as resource contributors and others, need to receive quality information. An important group of stakeholders includes banks, as they mobilise the guaranteed resources towards the final beneficiary. They require information that allows them to analyse the financial sustainability of the CGS and its ability to meet its commitments and comply with Basel III requirements if applicable.[5] In addition, even more relevantly, throughout the life cycle of the guarantee, banks and CGIs need to constantly share reliable and up-to-date information on the condition of the borrower they are helping to finance. In this crowded stage, the presence of a mechanism that standardises data and optimises information sharing may protect the interests of all stakeholders.

3   Selecting a Blockchain Configuration for CGS Support

This section discusses advantages and challenges that the adoption of blockchain platforms can bring within the CGS scenario.

Information stored on a ledger is tamper-proof, persistent, and non-repudiable. The layer of trust that blockchain infrastructures thereby provide is a key feature in potentially semi-trusted, competitive or untrusted multi-party business scenarios [26]. Therefore, they are apt for the case of a complex scenario such as that of CGS processes shown in Sect. 2. Furthermore, the

---

[5]European Central Bank: "Sound practices in Counterparty Credit Risk governance and management" (2023). www.bankingsupervision.europa.eu/legalframework/publiccons/pdf/ccr_report/ssm.ccrgovernancemanagement_202306.en.pdf

need to encode the cooperative behaviour of the system supporting CGSs call for the use of environments that support smart contracts. Existing mechanisms for the semi-automation of collaborative processes based on smart-contract enabled platforms provide a fertile ground for our specific use case [12,6]. As outlined in Sect. 2, finding a suitable platform category is a fundamental strategic decision to design a system based on blockchain [29]. In the following, we outline some key criteria guiding this choice in our context.

A **public permissionless** blockchain scheme like that of Ethereum and Algorand puts the secrecy of confidential data at risk and cannot be used in this scenario except with the necessary encryption of those reserved pieces of information. A common approach is to encrypt them via symmetric keys individually provided for readers [23,16]. However, this solution entails the additional overhead of managing keys at an individual level (which undermines scalability), keeping track of the shared ones (at the risk of breaching confidentiality), or having multiple duplicates of the same message with different encryptions (thus creating potential security issues caused by inconsistent copies). A promising alternative in that scenario is to decouple the attribution of keys from the individuals retaining them as proposed in the literature with frameworks such as Control Access via Key Encryption (CAKE) [20] and Multi-Authority Approach to Transaction Systems for Interoperating Applications MARTSIA [19]. These solutions, grounded in Attribute-Based Encryption (ABE) [4], resort to IPFS to store sensitive information and policies that determine data access based on the certified roles of the actors (e.g., whether an account is linked to a customer or not, a bank or not, and so forth). Data are thus encrypted and decrypted with keys that decouple the individuals from their access grants.

Public permissioned schemes (see, e.g., EOSIO[6]) have been developed to implement more restrictive consensus mechanisms on public networks. Public permissioned schemes suffer from the same issue as the public permissionless ones in terms of confidentiality constraints as the visibility of the transaction contents remains public. In addition, it may call for additional decision processes to decide who manages the ledger and leads consensus. Alternatively, organisations may opt for the implementation of private blockchains.

Private permissioned networks such as Hyperledger Fabric [1] exert control over the nodes with mechanisms including the verification of their actual identities, in line with the Know Your Customer (KYC) principles [21]. Platforms of this sort often include mechanisms for Role Based Access Control [3]. Another advantage of private blockchain networks is that the transaction costs, if any, are not bound to conversion into fiat currencies, as in the case of Ether, Algos, or Bitcoin, which is beneficial for limiting infrastructural costs. Only a subset of nodes participate in the consensus, so the content of the ledger is under the control of authoritative entities, too. These aspects are beneficial to preserve data confidentiality and system security. However, they demand an initial contracting phase and potentially conflicting subsequent management of who is in control of the ledger due to the permissioned nature of the infrastructure. In a setting such as that of CGSs, wherein a multitude of actors with cooperative scenarios and competing interests are involved, this situation might turn out to be undesirable.

Private permissionless blockchains, like LTO Network[7] have recently gained momentum. Similarly to the public permissionless setting, any node can take part in the consensus algorithm. However, unlike a public blockchain, only selected nodes are allowed to issue and read transactions. This hybrid nature is promising in our scenario as the distributed responsibility

---

[6]github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md
[7]ltonetwork.com

over the publication of transactions entails that no complex management procedures are in place to determine the entities in control of the ledger's content. At the same time, only nodes associated with certified actors enter the network. In our scenario, this implies that the exchanged information is accessible to the sole actors involved in the CGI.

4   Integrating Blockchain into the CGS Workflow

In this section, we represent the key stages of the credit guarantee life cycle, which includes three actors: *(i)* the borrower (the debtor of the loans or SMEs), *(ii)* the bank (the lender) and *(iii)* the Credit Guarantee Institution (CGI, the guarantor) [9]. In particular, we examine individual guarantee schemes, focusing on two specific aspects related to the timing of guarantee requests in relation to banks, namely whether these are requested ex-ante or ex-post. In these schemes, the CGI evaluates each loan application a lender submits to the bank either before (ex-ante) or after (ex-post). In Figures 1 to 3, we use flowcharts to highlight the key steps of the processes where the implementation of blockchain-based solutions can help improve efficiency and ensure process transparency. In addition, bell-shaped icons highlight the points where smart contracts may step in.

Figure 1 illustrates an example of an ex-ante application process. The smart contract and typical blockchain features can be adopted to seamlessly align with the **Know Your Customer (KYC)** [21] process required by the CGI, starting with the receipt of the application form. Smart contracts can automate, verify, and exchange KYC data safely and transparently by utilising certain configurations of blockchain-based distributed ledgers, allowing customers to submit their information.

Once stored on the blockchain, data cannot be altered or deleted, ensuring protection against fraud and unauthorised access. Furthermore, the network's interoperability can enable financial data sharing with the bank after the guarantee is accepted, enabling the loan application to be submitted. The smart contract can automate the sharing of KYC data between financial institutions, minimising the workload on both parties and maintaining compliance with cross-border requirements. Moreover, it can significantly speed up the KYC process, leading to quicker onboarding of new clients and lowering administrative costs, enhancing CGI's competitiveness. The contract code can automatically verify the information borrowers submit to approve the KYC status immediately without manual verification and indicate the absence of required additional data if need be. The CGI can efficiently interact with the borrower using a notification system based on the blockchain network. Upon compliance with the predefined rules and regulations of the smart contract (i.e., the successful outcome of the procedure), the automatic loan request can be submitted to the bank. This proposal focuses on applying blockchains to the CGI collateral issuance process. When considering bank valuation, interoperability must be deemed to allow all parties to participate in the blockchain network and possibly incorporate the loan provisioning procedure.

In the ex-post application process (Fig. 2), the bank first evaluates the loan application and the presence of sufficient collateral. The bank can expedite the inquiry process by sending the request directly to the CGI if necessary, as the borrower has already been checked and deemed eligible for the loan. In contrast with the ex-ante scenario, all subjects can be involved from the beginning. In this context, the effectiveness of blockchains and smart contracts depends on their ability to automate and optimise processes by exploiting the technology's unique characteristics and on the interoperability that would allow cooperation and data sharing between the different
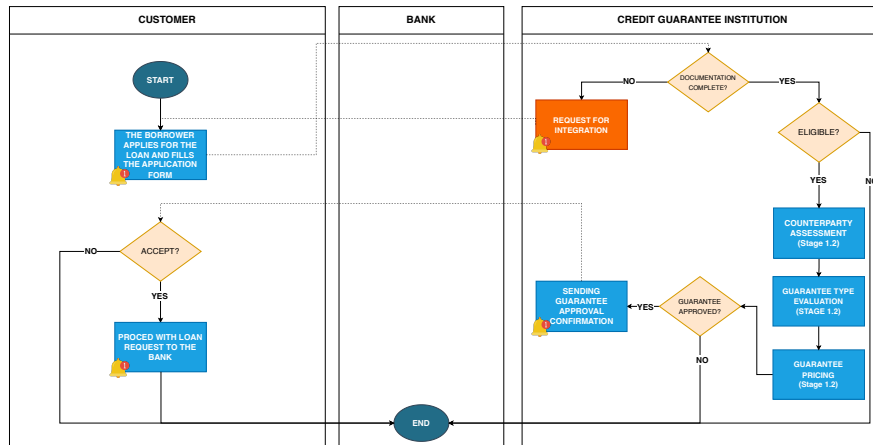
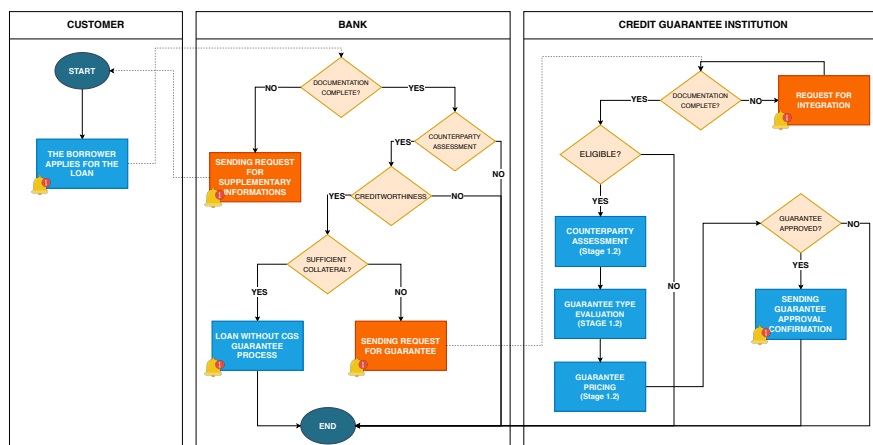Fig. 1: Individual Guarantee Scheme - Ex-ante application flowchart

Fig. 2: Individual Guarantee Scheme - Ex-post application flowchart

entities involved. Additionally, the immutability of DLTs improves openness and auditability among participants by recording KYC data on the blockchain, making it readily available to authorised parties. As with the ex-ante process, setting rules and regulations in the smart contract on the blockchain network can speed up the onboarding process by allowing the CGI to establish criteria in advance and verify them automatically. After the guarantee is approved and the risk-sharing agreement between the CGI and the bank has been achieved, the last condition to proceed with the loan disbursement is the guarantee fee payment verification. Once this condition has been respected, issuing the guarantee certificate is possible. As mentioned above in the flowcharts, in this stage, the platform's interoperability is essential since all the actors are involved in the process, and with advanced applications, it should be possible to integrate a smart loan contract. The smart contract previously deployed in Fig. 1 and Fig. 2 can also include this part of the process by assuming that the CGI approves the guarantee. As previously mentioned,
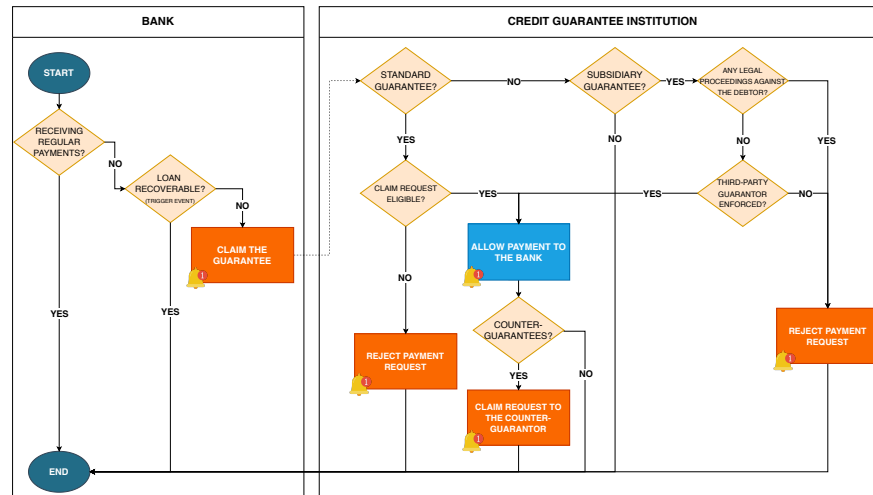
Fig. 3: Credit Guarantee Scheme - Enforcement

thanks to the smart contract preset rules and regulations, most of the process is completely automated, even if negotiating the line of risk conditions between the bank and the CGI requires human intervention. However, the exchange of documents and information between the parties involved is quick and secure, and all the subjects know the progress at any time.

Finally, when the loan contract starts, the bank begins the loan monitoring phase, verifying the regularity of payments and the ongoing creditworthiness of the SME and, if necessary, communicating any changes to the CGIs. As depicted in Fig. 3, the smart contract can be settled to enforce the guarantee if the trigger event occurs, such as when the borrower is unable or unwilling to repay as agreed in the guarantee contract. The smart contract has to predict the eligibility terms of the claim request by the bank according to the predetermined line of risk (the preestablished risk hierarchy). Knowing the risk line in case of default is crucial because if the bank can access the guarantee before other creditors, it may increase moral hazard, reducing the motivation to take action against the borrower. The smart contract can contain predefined conditions and encoded dispute resolution mechanisms. If legal enforcement is necessary, the contract will automatically initiate predefined actions, resulting in efficient and cost-effective resolutions compared to traditional guarantee enforcement. The potential of the blockchain network perfectly matches the need to check the legacy of legal enforcement in this stage more than in the previous onboarding stages. Notably, the fact that different stages of the enforcement process are continuous, transparent, and immutable on the blockchain makes it easier for everyone involved in the credit guarantee process to trust each other. This is because everyone can check the terms and conditions of the agreement and see how it is being carried out in real-time. Next, we conclude our paper with a summary and discussion of our findings.

5   Conclusion

This paper investigates the potential synergies between DLTs and CGSs by proposing a comprehensive framework for applying a blockchain to the credit guarantee life cycle. The

framework explores different stages of the process from the CGI's point of view, starting from the initial application to the potential enforcement, when the borrower is unable or unwilling to repay the loan and the bank claims the guarantee. We are unaware of any papers exploring the use of DLTs in the CGS process. We aim to initiate a new research direction by providing detailed information on the procedures, stakeholders, and data security in transactions. Additionally, we examine criteria to select a suitable DLT architecture that can enhance transparency, security, and automation in all stages of CGSs. We hypothesise to build a private permissionless blockchain that includes the actors involved in the CGS process. Considering the characteristics of this kind of blockchain compared to the public ones, only nodes associated with the certified actors can participate, ensuring the privacy of data in exchanging information. Secondly, we highlight how certain blockchain-based distributed ledger settings match the need to automate, verify, and share KYC data securely and transparently, proceeding without further manual intervention. This application could enhance the KYC process when onboarding a new borrower/guarantee application to the CGS blockchain network, making the process more effective and efficient. Moreover, implementing a blockchain network implies ease of use and communication between the borrower and the bank with the CGI. If the smart contract code's predefined rules and regulations are correctly observed, a slimmer process allows the borrower to easily proceed with the loan request to the bank (also thinking about the possibility of improving the interoperability of the network, including later a smart loan contract). This addresses the double-screening problem that significantly impacts the operational procedures of CGSs by allowing the CGI to establish essential criteria for the borrower's eligibility for the guarantee request. Our proposal suggests utilising the blockchain network to notify the guarantee institution when the enforcement trigger event occurs. At this stage, the CGI must determine if the bank's claim request meets the criteria based on the level of risk and legal enforcement history. The network's transparency allows all participants to monitor compliance with terms and conditions, accelerating the process and reducing moral hazard and irregularities.

References

1. Androulaki, E., Cachin, C., Caro, A.D., Sorniotti, A., Vukolic, M.: Permissioned blockchains and hyperledger fabric. ERCIM News (110) (2017)
2. Ayyagari, M., Demirguc-Kunt, A., Maksimovic, V.: Who creates jobs in developing countries? Small Business Economics **43**(1) (2014)
3. Baset, S.A., Desrosiers, L., Gaur, N., Novotny, P., O'Dowd, A., Ramakrishna, V.: Hands-on blockchain with Hyperledger: Building decentralized applications with Hyperledger Fabric and Composer. Packt Publishing Ltd (2018)
4. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: SP. pp. 321–334 (2007)
5. Chen, J., Micali, S.: Algorand: A secure and efficient distributed ledger. Theor. Comput. Sci. **777**, 155–183 (2019)
6. Corradini, F., Marcelletti, A., Morichetta, A., Polini, A., Re, B., Tiezzi, F.: A flexible approach to multi-party business process execution on blockchain. Future Gener. Comput. Syst. **147**, 219–234 (2023)
7. Corredera-Catalán, F., Pietro, F., Trujillo-Ponce, A.: Post-COVID-19 SME financing constraints and the credit guarantee scheme solution in Spain. Journal of Banking Regulation **22**(3), 250–260 (2021)

8. Dannen, C.: Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners. Apress (2017)
9. Deelen, L., Molenaar, K.: Guarantee Funds for Small Enterprises: A manual for guarantee fund managers. ILO (2004)
10. Demmou, L., Franco, G.: From hibernation to reallocation: Loan guarantees and their implications for post-covid-19 productivity (1687) (2021)
11. Di Ciccio, C.: Blockchain and Distributed Ledger Technologies, pp. 11–34. Cambridge University Press (2023)
12. Di Ciccio, C., Cecconi, A., Dumas, M., García-Bañuelos, L., López-Pintado, O., Lu, Q., Mendling, J., Ponomarev, A., Binh Tran, A., Weber, I.: Blockchain support for collaborative business processes. Informatik Spektrum **42**, 182–190 (2019)
13. Dirk A. Zetzsche, Linn Anker-Sørensen, M.L.P., Wehrli, A.: Dlt-based enhancement of cross-border payment efficiency – a legal and regulatory perspective. Law and Financial Markets Review **15**(1-2), 70–115 (2021)
14. de la Fuente-Cabrero, C., de Castro-Pardo, M., Santero-Sánchez, R., Laguna-Sánchez, P.: The Role of Mutual Guarantee Institutions in the Financial Sustainability of New Family-Owned Small Businesses. Sustainability **11**(22), 1–15 (2019)
15. Gervais, A., Karame, G.O., Wüst, K., Glykantzis, V., Ritzdorf, H., Capkun, S.: On the security and performance of proof of work blockchains. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. p. 3–16. Association for Computing Machinery, New York, NY, USA (2016)
16. Ghayvat, H., Pandya, S., Bhattacharya, P., Zuhair, M., Rashid, M., Hakak, S., Dev, K.: CP-BDHCA: Blockchain-based confidentiality-privacy preserving big data scheme for healthcare clouds and applications. IEEE Journal of Biomedical and Health Informatics **26**(5), 1937–1948 (2022)
17. Haskell, C.D.: Institutional research as a bridge: Aligning institutional internal data needs and external information requirements a strategic view. Higher Education Evaluation and Development **11**(1), 2–11 (2017)
18. Leone, P., Panetta, I.C., Porretta, P.: Credit Guarantee Institutions, Performance and Risk Analysis: An Experimental Scoring, pp. 115–160. Palgrave Macmillan UK (2013)
19. Marangone, E., Di Ciccio, C., Friolo, D., Nemmi, E.N., Venturi, D., Weber, I.: MARTSIA: Enabling data confidentiality for blockchain-based process execution. In: EDOC. pp. 58–76 (2023)
20. Marangone, E., Di Ciccio, C., Weber, I.: Fine-grained data access control for collaborative process execution on blockchain. In: BPM Blockchain and RPA Forum. pp. 51–67 (2022)
21. Moyano, J.P., Ross, O.: KYC optimization using distributed ledger technology. Bus. Inf. Syst. Eng. **59**(6), 411–423 (2017)
22. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008)
23. National Institute of Standards and Technology: Announcing the Advanced Encryption Standard (AES). Tech. rep., Federal Information Processing Standards Publication 197 (2001)
24. Nguyen, C.T., Hoang, D.T., Nguyen, D.N., Niyato, D., Nguyen, H.T., Dutkiewicz, E.: Proof-of-stake consensus mechanisms for future blockchain networks: Fundamentals, applications and opportunities. IEEE Access **7**, 85727–85745 (2019)
25. Schich, S., Cariboni, J., Naszodi, A., Maccaferri, S.: Evaluating publicly supported credit guarantee programmes for SMEs. OECD (2017)
26. Weber, I., Xu, X., Riveret, R., Governatori, G., Ponomarev, A., Mendling, J.: Untrusted business process monitoring and execution using blockchain. In: BPM. Lecture Notes in Computer Science, vol. 9850, pp. 329–347. Springer (2016)
27. Wood, G.: Ethereum: A secure decentralised generalised transaction ledger (2014)
28. World Bank Group: Principles for public credit guarantee schemes for smes. Working Paper 101769 (2015)
29. Wüst, K., Gervais, A.: Do you need a blockchain? In: CVCBT. pp. 45–54 (2018)

References

Leo, Sabrina, Andrea Delle Foglie, Luca Barbaro, Edoardo Marangone, Ida Claudia Panetta, and
Claudio Di Ciccio (2024). "Transforming Credit Guarantee Schemes with Distributed Ledger Tech-
nology". In: *ICBT*. Ed. by Bahaaeddin Alareeni and Allam Hamdan. Vol. 1083. Lecture Notes in
Networks and Systems. Springer, pp. 314–324. ISBN: 978-3-031-67431-0. DOI: 10.1007/978-3-
031-67431-0_30.

BibTeX

```
@InProceedings{  Leo.etal/ICBT2024:TransformingCGSWithDLT,
  author        = {Leo, Sabrina and Delle Foglie, Andrea and Barbaro, Luca
                   and Marangone, Edoardo and Panetta, Ida Claudia and Di
                   Ciccio, Claudio},
  booktitle     = {ICBT},
  title         = {Transforming Credit Guarantee Schemes with Distributed
                   Ledger Technology},
  year          = {2024},
  pages         = {314--324},
  publisher     = {Springer},
  crossref      = {ICBT2024},
  doi           = {10.1007/978-3-031-67431-0_30},
  keywords      = {Distributed Ledger Technologies; Blockchain; CGS; SME
                   Finance}
}
@Proceedings{   ICBT2024,
  title         = {Transforming Credit Guarantee Schemes with Distributed
                   Ledger Technology},
  year          = {2024},
  editor        = {Alareeni, Bahaaeddin and Hamdan, Allam},
  isbn          = {978-3-031-67431-0},
  publisher     = {Springer},
  series        = {Lecture Notes in Networks and Systems},
  volume        = {1083},
  booktitle     = {Navigating the Technological Tide: The Evolution and
                   Challenges of Business Model Innovation, ICBT 2024,
                   Cambridge, UK, April 19-20, 2024, Proceedings}
}
```