Blockchain-Based Systems Development Using Model-Driven Engineering

Gislainy Velasco[1], Noeli Antônia Pimentel Vaz[1,2],
Matheus Brito Martins[1], Matheus Lázaro Honório da Silva[1],
Pedro Moraes Ribeiro Gonçalves Silva[1], Sergio T. Carvalho[1]

[1]Instituto de Informática – Universidade Federal de Goiás (UFG)
Caixa Postal 131 — 74001-970 — Goiânia — GO -– Brasil

[2]Instituto Acadêmico de Ciências Exatas e Tecnológicas – Universidade Estadual de Goiás (UEG)
Caixa Postal 459 — 75132-903 — Anápolis — GO — Brasil

{gislainycrisostomo, noelivaz}@discente.ufg.br

{matheus.b.m, matheus.lazaro, pedro_ribeiro}@discente.ufg.br

sergiocarvalho@ufg.br

Abstract. *Blockchain-based software development faces significant challenges related to decentralization, coordinating system elements across network nodes, and making complex decisions about the distribution of software components between blockchain and conventional structures. Additionally, the limitation in data storage capacity in blockchain transactions requires integrating solutions, raising critical access control issues, and removing false or legally problematic data when stored on the ledger. Identity management also undergoes transformations, with users being identified by encrypted addresses and their interactions validated by private access keys, presenting security and information recovery challenges in case of private key loss. The integration between blockchains and conventional systems becomes essential to ensure the architectural integrity of the systems. In this context, an approach is introduced for developing blockchain-based systems, focusing on integrating conventional systems through Model-Driven Engineering (MDE). The central proposal aims to fill a gap in the literature, providing a comprehensive strategy from conception to implementation in blockchain-based systems, using MDE as a software engineering technique. This work is presented as a position paper, representing an ongoing effort outlining an innovative perspective in blockchain systems development. This exploratory research project investigates potential synergies between blockchain and MDE techniques. We hope to contribute significantly to the seamless integration between blockchain and conventional systems.*

1. Introduction

The blockchain technology has emerged as an innovation that is bringing about substantial transformations in how software systems are conceived. Its features, such as privacy, transparency, decentralization, and immutability, offer remarkable potential for applications across a wide range of sectors [Angelis and Ribeiro da Silva 2019, Khan et al. 2019, Six et al. 2022]. In the healthcare sector, for instance, the inherent immutability of blockchain ensures the integrity and security of patients' medical records, preventing any undesired manipulation. Similarly, in supply chain management, the ability to accurately trace all transactions of a product from its origin to the end consumer provides complete transparency and assists in fraud reduction. Other areas, such as financial services, logistics, electronic voting, and intellectual property, have also embraced blockchain-based systems to enhance the reliability and security of their operations.

Blockchain is a distributed ledger technology that allows participants to record transactions irreversibly. Its fundamental characteristic lies in data immutability, ensuring stored information's integrity and reliability. The blockchain operation occurs in a decentralized or partially decentralized network. The validation and recording of transactions on the blockchain are accomplished through a consensus algorithm, ensuring that all participants agree on the current state of the network. This makes it resistant to censorship attempts and isolated failures, providing transparency and transaction security. There are various types of blockchains, including public ones like Bitcoin [Nakamoto 2008] and Ethereum [Buterin et al. 2014], which are open-access and permissioned ones that restrict access to authorized participants. Additionally, private blockchains are controlled by a single entity or consortium, such as Hyperledger Fabric.

The blockchain technology has been integrated into conventional software systems, incorporating essential elements such as smart contracts, enabling the direct execution of system logic on the blockchain. In this way, systems introduce a new source of trust, not necessarily relying solely on information stored in their internal databases but rather depending on the current state of the blockchain network as the primary source of truth. In this context, applications utilizing blockchain face new challenges, notably immutability, which in certain cases makes the alteration process a challenging task [Velasco et al. 2023a]. Additionally, consensus algorithms also substantially impact system architecture, primarily due to their crucial role in maintaining the integrity and reliability of the network. These challenges, inherent in blockchain adoption, drive the need for innovative approaches in developing systems based on this technology.

Given these complexities inherent in blockchain applications, there is a pressing need for structured approaches that can manage these intricacies effectively. Model-driven engineering (MDE) emerges as a potent technique, offering robust tools for designing, simulating, and validating the architectural integrity of blockchain-based systems before their actual implementation [Seidewitz 2003]. The synergy between MDE and blockchain is grounded in the ability of MDE to abstract higher levels of system complexity into manageable models, which can be directly translated into executable smart contracts, enhancing both the development process and maintenance lifecycle of blockchain applications.

Several studies have focused on automating the development of smart contracts, aiming to empower individuals to create and deploy their smart contracts on a blockchain network [Teles-Borges et al. 2024, Hamdaqa et al. 2022, Qasse et al. 2021, Velasco et al. 2023b, Velasco et al. 2023c]. MDE is one of the prominent software engineering techniques in the development of contracts [Barišić et al. 2021, Jurgelaitis et al. 2022, Tsai et al. 2019, Qasse et al. 2021]. However, comprehensive software system modeling remains an issue that needs attention. In some cases, the system is not considered as a whole, neglecting aspects that include client, server, deployment, maintenance, and all stages involved in conventional software development.

The central purpose of this position paper is to delve into the analysis of inherent complexities in the comprehensive development of blockchain-based systems. This approach represents an extension of research from a previous that outlined a model-driven strategy for smart contract development [Velasco et al. 2023a, Velasco et al. 2023b, Velasco et al. 2023c, Velasco 2023]. In this context, the emphasis is on expanding this approach and investigating how it can be holistically applied in constructing blockchain-based software systems. The primary goal is to foster a comprehensive understanding of the development of these systems, considering all elements involved in their conception and implementation while also exploring challenges, identifying emerging trends, and highlighting relevant research issues.

The remaining sections of this paper are structured as follows: in Section 2, the justifications for conducting research in blockchain-based systems development are presented. Section 3 discusses related works in the blockchain and smart contract development domain that leverage some MDE techniques. Subsequently, in Section 4, the objectives of this paper are outlined, considering it as an ongoing research idea. Finally, in Section 5, concluding remarks are presented, addressing the research on this theme and the expected contributions.

2. Justification

As the adoption of blockchain expands across sectors such as healthcare, finance, logistics, and others, the need to develop software systems that fully harness the potential of blockchain becomes evident [Six et al. 2022]. This encompasses aspects such as the overall system architecture, interactions between different components, system integrations, ensuring security, and regulatory compliance, among others.

As the blockchain components integrate with other system elements, the architecture's complexity becomes even more apparent [Barbaria et al. 2023]. An example is the influence of the blockchain's consensus algorithm on transactions originating from external systems. These systems may need to adapt quickly to the constantly changing state of the network if a transaction is invalidated by the consensus algorithm [Viriyasitavat and Hoonsopon 2019]. This introduces an additional layer of complexity in managing the system architecture.

Furthermore, conventional systems, understood here as systems that do not utilize blockchain, often adopt a centralized logic structure where all operations are executed internally. However, incorporating smart contracts redefines this approach, requiring specialized management [Velasco et al. 2023a]. Such a transformation implies that developers must meticulously consider the interaction of these contracts with the system as a whole, introducing a new layer of complexity to the overall architecture.

Other issues that arise during the blockchain software development process concern decentralization. The distribution of system elements across nodes in the network brings forth challenges related to coordination and communication, aspects not typically confronted in centralized architectures. Decision-making regarding which parts of the software should reside on the blockchain and which should remain in conventional structures also proves to be a complex dilemma, requiring careful assessments of effectiveness, security, and feasibility of such implementation [Six et al. 2022].

Blockchain-based systems also face challenges related to the storage of voluminous data, as the current structure of blockchain transactions does not allow for the storage of extensive information, necessitating the incorporation of other elements such as the InterPlanetary File System (IPFS) [Deepa et al. 2022]. This raises critical issues of access control to information and, in some cases, the need to remove data from the network due to falsehoods or legal implications. Therefore, there is a need to design systems that consider these complexities, ensuring the proper integration of software elements into any system without compromising its architectural integrity.

Furthermore, these types of systems introduce new approaches to identity management, where users are identified through encrypted addresses, and their interactions on the network are verified through their private access keys [Yang and Li 2020]. This approach involves pseudonymizing users' identities, turning them into cryptographic pseudonyms rather than directly identifiable personal information. However, this also poses significant challenges in digital identity management, as the loss of the private key results in irrecoverability, making the use of brute-force algorithms unfeasible for retrieval. Consequently, blockchain systems face emerging challenges in digital identities, requiring solutions to ensure users can securely manage their information on the network. In this context, it is crucial to consider the incorporation of this new identification model into conventional systems.

Given the complexities introduced by blockchain, MDE can offer significant tools for system development. Although the direct integration of MDE in blockchain environments is still in an exploratory phase, its abstraction and detailed modeling capabilities hold promise for addressing architectural and operational challenges. MDE has the potential to facilitate the simulation of complex scenarios and the validation of architectures before actual implementation, providing a platform to refine design decisions and ensure system integrity [Curty et al. 2023]. The promising area of research here lies in exploring how MDE can be specifically applied to develop systems that integrate blockchain technology rather than focusing on advancing the technologies of MDE or blockchain themselves.

3. Literature Review

Since the first generation of blockchain, symbolized by the advent of Bitcoin [Nakamoto 2008], various researchers have explored the potential of this technology in their respective fields of study, owing to its characteristics of immutability, transparency, security, and anonymity. With the emergence of Ethereum [Buterin et al. 2014], which enabled the implementation of smart contracts on its virtual machine, new possibilities for application emerged, integrating smart contracts as essential components in a variety of contexts. These studies encompass the use of blockchain as a means to achieve specific goals, as well as contributions to the ongoing development of the technology, whether through the development of tools or collaboration with the core of the technology itself.

The application of blockchain technology spans various domains. In the healthcare sector, for instance, the technology is employed to ensure the integrity and security of data [Ghosh et al. 2023]. In the supply chain, blockchain is used to track the entire production process [Pournader et al. 2020]. Additionally, in the Internet of Things (IoT)-related projects, blockchain is crucial in ensuring data reliability and protection [Alladi et al. 2019]. In banking and financial systems, blockchain eliminates the need for a trusted third party, with cryptocurrencies serving as a means of value exchange [Chowdhury et al. 2021]. Moreover, blockchain technology also finds application in governmental systems, contributing to the enhancement of governance [Carter and Ubacht 2018].

As a consensus among researchers, blockchain technology poses significant challenges. In our previous work outlined in [Velasco et al. 2023a], we conducted a literature review that identified critical challenges faced by smart contract developers throughout their development cycle and the broader challenges presented by the technology in this area. Building upon these findings, we have developed a model-driven approach to make the smart contract modeling process more intuitive for stakeholders, as discussed in [Velasco et al. 2023c, Velasco 2023]. Further extending this work, we created a graphical tool for modeling smart contracts for the Ethereum Virtual Machine, detailed in [Velasco et al. 2023b].

In the context of developing blockchain-based systems, [Curty et al. 2023] presents a detailed analysis of the use of MDE, low-code, and no-code platforms to facilitate the creation of blockchain applications. This study conducts a structured literature review, comparing academic and industrial approaches to highlight the technical complexities involved and how these can be abstracted to broaden the adoption of blockchain technologies in the business sector. One of the key points emphasized is the potential of low/no-code platforms to simplify the development process, allowing even users with limited programming knowledge to create robust applications. This work identifies several research opportunities, such as the need to develop new approaches that integrate MDE more effectively into low/no-code platforms, aiming at the optimization and efficiency of blockchain applications. The relevance of this study to current research lies in its comparative and analytical approach, which clarifies the current state of MDE usage in blockchain applications and suggests paths for future investigations that could strengthen and expand the applicability of this disruptive technology.

In the field of smart contract development, various efforts are underway to enhance and innovate the modeling and implementation of these contracts. Approaches based on Model-Driven Engineering (MDE) and Model-Driven Architecture (MDA) have been applied in projects to simplify contract creation. For instance, some studies have proposed chatbots employing natural language to model contracts [Hamdaqa et al. 2022, Qasse et al. 2021], while others have explored *multichain* contract structures to address reliability issues [Barišić et al. 2021]. Furthermore, MDE-based frameworks have been developed to generate legal contract models and transform them into Solidity code specific to the Ethereum platform [Jurgelaitis et al. 2022, Tsai et al. 2019]. In [Teles-Borges et al. 2024], Jabuti CE is introduced, a tool implemented as an extension for Visual Studio Code. This tool enables the modeling of smart contracts through the Jabuti DSL, providing the ability to specify platform-independent contracts for Enterprise Application Integration.

Other approaches include tools enabling the runtime writing of contracts using JSON and Typescript models [Santiago et al. 2021], as well as frameworks employing *patching* mechanisms to repair already deployed contracts [Jin et al. 2022]. Solutions involving UML state diagrams in contract generation are also explored [Garamvölgyi et al. 2018, Jurgelaitis et al. 2022], along with tools for writing formally verified contracts [Tsai et al. 2019]. These endeavors showcase a variety of innovative approaches and techniques to tackle the challenges of smart contract development.

In other works, a software architectural concern is evident. In [Barbaria et al. 2023], an architectural model was introduced to integrate blockchain technology into the healthcare industry using Hyperledger Fabric. The solution was designed to manage sensitive health data across various healthcare and research institutions, ensuring the security of this sensitive data through a decentralized paradigm that demonstrates resilience to current cyber threats.

4. Goal

This position paper presents a proposal to facilitate the development of blockchain-based systems by applying MDE. The main goal is to develop a clear and efficient methodology that can be applied to simplify the creation of these blockchain-based systems. Initially, we have defined a series of specific objectives. The first step is to conduct exploratory research to gain a deep understanding of the blockchain domain and its intersection with conventional software systems. This initial phase is crucial for identifying specific needs and the technical complexities that MDE needs to address.

After the exploratory research, we will focus on a comprehensive study of the intrinsic complexities of developing blockchain-based systems, covering the conceptual and implementation phases. This study will include formulating the theoretical and practical bases necessary to develop blockchain systems effectively. Furthermore, our scope will include the development of specific approaches that enable efficient modeling of these systems. These approaches will be tested through case studies in different usage scenarios to validate their practical applicability.

Finally, we intend to ensure the quality of the proposed approaches through collaborative evaluations with external users, ensuring that they effectively meet the needs of blockchain-based software systems according to predefined quality metrics. We acknowledge that this project is still in its exploratory phase. As part of our future objectives, we are designing a model to serve as a reference for implementing blockchain systems using MDE principles. This model will be detailed later in the project development to provide a robust and adaptable framework for future development.

5. Final Remarks

Blockchain technology has proven to be a powerful tool for developing and enhancing software systems. It has been studied in various contexts, both in academia and industry. This article acknowledges this reality and emphasizes the need for further exploration in blockchain-based systems development. Consequently, significant results are anticipated through this research.

One of the most significant contributions lies in establishing seamless integration between blockchain-based and conventional software systems. This contribution is expected to enable the widespread adoption of blockchain technology in various real-world contexts. The research will contribute to advancing scientific knowledge by filling gaps in existing literature and identifying new approaches at the intersection of blockchain and systems modeling. As the research findings translate into applicable practices and tools, they are expected to positively impact the software development and blockchain industry, allowing companies and organizations to enhance their blockchain-based systems.

Regarding when these results can be expected, the project is structured in phases, with preliminary results anticipated within the next 12 months. Following the initial phase, further refinements and additional case studies will be conducted, aiming for a comprehensive rollout of findings and practical applications within the next 24 to 36 months. This timeline depends on ongoing collaborations and the continuous adaptation of our methodologies to emerging challenges and opportunities within the field.

References

[Alladi et al. 2019] Alladi, T., Chamola, V., Parizi, R. M., and Choo, K.-K. R. (2019). Blockchain Applications for Industry 4.0 and Industrial IoT: A Review. *IEEE Access*, 7:176935–176951.

[Angelis and Ribeiro da Silva 2019] Angelis, J. and Ribeiro da Silva, E. (2019). Blockchain adoption: A value driver perspective. *Business Horizons*, 62(3):307–314.

[Barbaria et al. 2023] Barbaria, S., Mahjoubi, H., and Rahmouni, H. B. (2023). A novel blockchain-based architectural modal for healthcare data integrity: Covid19 screening laboratory use-case. *Procedia Computer Science*, 219:1436–1443.

[Barišić et al. 2021] Barišić, A., Zhu, E., and Mallet, F. (2021). Model-driven approach for the design of Multi-Chain Smart Contracts. In *2021 3rd BRAINS)*, pages 37–38.

[Buterin et al. 2014] Buterin, V. et al. (2014). A next-generation smart contract and decentralized application platform. *white paper*, 3(37):2–1.

[Carter and Ubacht 2018] Carter, L. and Ubacht, J. (2018). Blockchain applications in government. In *Proceedings of the 19th Annual International Conference on Digital Government Research: governance in the data age*, pages 1–2.

[Chowdhury et al. 2021] Chowdhury, M. U., Suchana, K., Alam, S. M. E., and Khan, M. M. (2021). Blockchain application in banking system. *Journal of Software Engineering and Applications*, 14(7):298–311.

[Curty et al. 2023] Curty, S., Härer, F., and Fill, H.-G. (2023). Design of blockchain-based applications using model-driven engineering and low-code/no-code platforms: a structured literature review. *Software and Systems Modeling*, 22(6):1857–1895.

[Deepa et al. 2022] Deepa, N., Pham, Q.-V., Nguyen, D. C., Bhattacharya, S., Prabadevi, B., Gadekallu, T. R., Maddikunta, P. K. R., Fang, F., and Pathirana, P. N. (2022). A survey on blockchain for big data: Approaches, opportunities, and future directions. *Future Generation Computer Systems*, 131:209–226.

[Garamvölgyi et al. 2018] Garamvölgyi, P., Kocsis, I., Gehl, B., and Klenik, A. (2018). Towards Model-Driven Engineering of Smart Contracts for Cyber-Physical Systems. In *2018 48th Annual IEEE/IFIP DSN-W*, pages 134–139.

[Ghosh et al. 2023] Ghosh, P. K., Chakraborty, A., Hasan, M., Rashid, K., and Siddique, A. H. (2023). Blockchain Application in Healthcare Systems: A Review. *Systems*, 11(1).

[Hamdaqa et al. 2022] Hamdaqa, M., Met, L. A. P., and Qasse, I. (2022). iContractML 2.0: A domain-specific language for modeling and deploying smart contracts onto multiple blockchain platforms. *Information and Software Technology*, 144:106762.

[Jin et al. 2022] Jin, H., Wang, Z., Wen, M., Dai, W., Zhu, Y., and Zou, D. (2022). Aroc: An Automatic Repair Framework for On-Chain Smart Contracts. *IEEE Transactions on Software Engineering*, 48(11):4611–4629.

[Jurgelaitis et al. 2022] Jurgelaitis, M., čeponienė, L., and Butkienė, R. (2022). Solidity Code Generation From UML State Machines in Model-Driven Smart Contract Development. *IEEE Access*, 10:33465–33481.

[Khan et al. 2019] Khan, A. G., Zahid, A. H., Hussain, M., Farooq, M., Riaz, U., and Alam, T. M. (2019). A journey of WEB and Blockchain towards the Industry 4.0: An Overview. In *2019 International Conference on Innovative Computing (ICIC)*, pages 1–7.

[Nakamoto 2008] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, page 21260.

[Pournader et al. 2020] Pournader, M., Shi, Y., Seuring, S., and Koh, S. L. (2020). Blockchain applications in supply chains, transport and logistics: a systematic review of the literature. *International Journal of Production Research*, 58(7):2063–2081.

[Qasse et al. 2021] Qasse, I., Mishra, S., and Hamdaqa, M. (2021). iContractBot: A Chatbot for Smart Contracts' Specification and Code Generation. In *2021 IEEE/ACM 3rd BotSE*, pages 35–38.

[Santiago et al. 2021] Santiago, L., Abijaude, J., and Greve, F. (2021). A Framework to Generate Smart Contracts On the Fly. In *Proceedings of the XXXV SBES*, page 410–415, New York, NY, USA. Association for Computing Machinery.

[Seidewitz 2003] Seidewitz, E. (2003). What models mean. *IEEE Software*, 20(5):26–32.

[Six et al. 2022] Six, N., Herbaut, N., and Salinesi, C. (2022). Blockchain software patterns for the design of decentralized applications: A systematic literature review. *Blockchain: Research and Applications*, 3(2):100061.

[Teles-Borges et al. 2024] Teles-Borges, M., Bocanegra, J., Dornelles, E. F., Sawicki, S., Reina-Quintero, A. M., Molina-Jimenez, C., Roos-Frantz, F., and Frantz, R. Z. (2024). Jabuti CE: A Tool for Specifying Smart Contracts in the Domain of Enterprise Application Integration. In *MODELSWARD24*.

[Tsai et al. 2019] Tsai, W.-T., Ge, N., Jiang, J., Feng, K., and He, J. (2019). Invited Paper: Beagle: A New Framework for Smart Contracts Taking Account of Law. In *2019 IEEE SOSE*, pages 134–13411.

[Velasco et al. 2023a] Velasco, G., Vaz, N., and Carvalho, S. (2023a). Challenges and Opportunities in Smart Contract Development on the Ethereum Virtual Machine. In *Proceedings of the 6th Blockchain Workshop: Theory, Technology and Applications*, pages 15–28, Porto Alegre, RS, Brazil. SBC.

[Velasco et al. 2023b] Velasco, G., Vieira, D., Vieira, M., and Carvalho, S. (2023b). SCMTool: A Graphical Tool for Smart Contract Modeling. In *Proceedings of the 1st Colloquium on Blockchain and Decentralized Web*, pages 31–36, Porto Alegre, RS, Brazil. SBC.

[Velasco et al. 2023c] Velasco, G., Vieira, M., and Carvalho, S. (2023c). Evaluation of a High-Level Metamodel for Developing Smart Contracts on the Ethereum Virtual Machine. In *Proceedings of the 6th Blockchain Workshop: Theory, Technology and Applications*, pages 29–42, Porto Alegre, RS, Brasil. SBC.

[Velasco 2023] Velasco, G. C. (2023). A Model-Driven Approach to Smart Contract Development (in portuguese). *Master dissertation - Instituto de Informática, Universidade Federal de Goiás*.

[Viriyasitavat and Hoonsopon 2019] Viriyasitavat, W. and Hoonsopon, D. (2019). Blockchain characteristics and consensus in modern business processes. *Journal of Industrial Information Integration*, 13:32–39.

[Yang and Li 2020] Yang, X. and Li, W. (2020). A zero-knowledge-proof-based digital identity management scheme in blockchain. *Computers & Security*, 99:102050.