Cerdika: Jurnal Ilmiah Indonesia, 6 (2), 2026
p-ISSN: 2774-6291 e-ISSN: 2774-6534

Available online at http://cerdika.publikasiindonesia.id/index.php/cerdika/index

The Role of Informatics Engineering in the Development of Digital Assets as an Alternative Solution Amid Economic Crisis

Natalia Artha Malau[1] , Jeovano Lorensius Mamesah[2] , Citra Resky Kabolo[3] , Christiany Cheerel Runturambi[4] , Fadel Dasilva Sumaga[5]
Politeknik Negeri Manado, Indonesia[1,2,3,4,5]
Email: nataliamalau@unima.ac.id[1], jeovanomamesah05@gmail.com[2], citraresky17@gmail.com[3], cristianyrunturambi@gmail.com[4], sumagafadel15@gmail.com[5]

Abstract
The current economic crisis affecting multiple sectors demands digital technology innovations as effective and efficient alternative solutions. This study examines how informatics engineering can contribute to the development of blockchain-based digital assets, particularly through the utilization of cryptocurrency, NFTs, and the simulation of Central Bank Digital Currency (CBDC). The research adopts an implementation-based approach by developing digital assets through a series of stages, including a literature review, needs analysis, system design, and functional evaluation. The findings show that blockchain-based digital assets can provide secure, transparent, and inclusive solutions as an alternative for economic reinforcement amid crisis conditions. The study implies that strategic collaboration among academics, technology developers, financial institutions, and regulators is essential to create an inclusive, efficient, and sustainable digital asset ecosystem that can contribute to national economic resilience.

Keywords: Informatics Engineering; Digital Assets; Blockchain; Cryptocurrency; NFT

INTRODUCTION

The current global economic crisis is driven by multiple complex factors, such as the prolonged effects of the pandemic, geopolitical tensions, rising inflation, and fluctuations in global commodity prices. These conditions have weakened economic stability in many countries, including Indonesia, leading to declining productivity, reduced purchasing power, and increasing unemployment. According to Hidayat (2020), global economic uncertainty demands technological innovations capable of providing new solutions for maintaining economic sustainability in the digital era.

In this context, informatics engineering plays a critical role in creating digital solutions that address modern economic challenges. One of the most influential innovations is the implementation of blockchain technology, which forms the foundation for various digital assets such as cryptocurrency, non-fungible tokens (NFTs), and Central Bank Digital Currency (CBDC) (CBDC, 2025; Chairunnas & Sugianto, 2024; Collberg & Davidson, 2011; Guliyev & Bethlendi, 2026; Institute, 2025; Shameli-Sendi & Aghababaei-Barzegar, 2016). Blockchain offers transparency, security, and decentralization, reducing dependence on traditional financial institutions that often struggle during times of crisis (D. Sari & Rahman, 2021).

Digital assets such as cryptocurrency have become symbols of major change in the global financial system (Fund, 2025; International, 2025; Yermack, 2017). According to Yuliana (2022), cryptocurrencies have the potential to act as a store of value and as investment instruments due to their efficiency, speed, and borderless characteristics. Moreover, blockchain-based financial systems promote financial inclusion by enabling access for

communities underserved by conventional banking systems (Crosby et al., 2016; Tapscott & Tapscott, 2016).

Furthermore, the development of digital assets cannot be separated from the role of informatics engineering in strengthening cybersecurity, data integrity, and transaction system reliability. Pratama (2021) emphasized that the implementation of cryptographic algorithms and machine-learning-based threat detection plays a vital role in enhancing public trust in digital financial systems. Therefore, synergy among technology developers, government institutions, and the public becomes essential in building a safe, adaptive, and sustainable digital ecosystem (Wesselbaum, 2020).

The urgency of this research is underscored by the escalating economic pressures and the rapid, often unregulated, growth of the digital asset market in Indonesia and globally. Millions of Indonesians are already engaging with cryptocurrencies, driven by a search for alternative investments and financial inclusion. However, this participation occurs within a landscape characterized by significant risks, including extreme price volatility, cybersecurity threats, and regulatory uncertainty (Yuliana, 2022; Pratama, 2021). A clear, research-based understanding of how informatics engineering can contribute to building secure, reliable, and beneficial digital asset systems is therefore not just an academic pursuit but a critical necessity for protecting consumers, informing sound policy, and harnessing the potential of this technology for national economic resilience.

The novelty of this research lies in its integrated, multi-faceted approach. It combines a theoretical review of blockchain technology and digital assets with a practical, implementation-based component, including the creation of an account on a real-world cryptocurrency exchange (INDODAX) to simulate transactions. This hands-on element grounds the theoretical discussion in practical reality. Furthermore, the study explicitly links the technical discussion of blockchain architecture, cryptographic security, and system design to the broader socio-economic context of an economic crisis and the specific regulatory landscape of Indonesia. By doing so, it moves beyond abstract discussions to provide a contextualized analysis of the potential and challenges of digital assets as an alternative economic solution.

The primary purpose of this research is to examine the role of informatics engineering in the development of blockchain-based digital assets, with a specific focus on their potential as an alternative solution during an economic crisis. The research objectives are: (1) to explore the fundamental concepts and technologies underpinning digital assets, including blockchain, cryptocurrency, NFTs, and CBDCs; (2) to demonstrate the practical application of informatics engineering principles through the simulation of cryptocurrency transactions; (3) to analyze the potential benefits and inherent risks of digital assets, particularly in the context of an economic downturn; and (4) to discuss the implications of these technologies for Indonesia, considering aspects of security, regulation, and digital literacy.

Based on the above explanation, this study aims to examine the role of informatics engineering in the development of cryptocurrency as an alternative solution during an economic crisis. This research is expected to contribute to strengthening the utilization of information technology in digital finance, especially in aspects of security, efficiency, and its potential application in Indonesia, which is transitioning toward a digital-based economy.

METHOD

Data collection involved literature studies related to blockchain, cryptocurrency, NFTs, and CBDC. An INDODAX account was also created as a tool for executing buy-and-sell crypto transactions.

This research adopts a design and development approach to explore the contribution of informatics engineering in building blockchain-based digital assets as alternative economic solutions. The methodology is structured into four main stages: literature review, system design, prototyping, and functional evaluation. The literature review synthesizes contemporary academic and industry sources concerning blockchain architecture, cryptocurrency mechanisms, smart contracts, and the emerging concept of Central Bank Digital Currency (CBDC). This stage establishes the theoretical foundation and identifies technical gaps that inform the system design phase, ensuring alignment with both user needs and security standards.

Functional evaluation is carried out through black-box testing and scenario-based simulations to assess system performance, transaction speed, security features, and user accessibility. Evaluation metrics include transparency of ledger updates, resistance to basic manipulation attempts, and ease of interaction for non-technical users. The findings from this evaluation are analyzed qualitatively to determine the viability and limitations of the proposed system. This multi-stage methodology allows the research to not only propose technical solutions but also to reflect critically on the socio-economic implications of deploying digital assets during periods of economic instability.

RESULTS AND DISCUSSION

The role of informatics engineering in developing cryptocurrency demonstrates that these digital assets can serve as viable alternatives during an economic crisis. They enable easier and faster access to financial services and offer potential financial gains. Digital assets like cryptocurrencies can help communities preserve asset value amid current economic instability.

Innovations in informatics engineering have transformed the financial system through technologies such as blockchain and cryptography, which serve as the foundation of digital assets like cryptocurrencies. Blockchain operates on a decentralized network, meaning transaction records are distributed across multiple computers, making data manipulation significantly more difficult. As stated by (S. A. Sari & Nasution, 2023), blockchain's transparent and secure nature enables digital transactions to occur without the need for banks or intermediary financial institutions. This empowers individuals worldwide to access and transfer digital assets globally, opening broader opportunities for financial inclusion.

From an economic perspective, digital assets such as cryptocurrency are increasingly viewed as alternatives during global uncertainty. (Hidayat, 2020) explains that while traditional financial instruments are affected by inflation, currency fluctuations, and erratic monetary policy, digital assets provide alternative investment options. They offer flexible capital, efficient transaction processes, and broader accessibility, which are particularly appealing to younger generations familiar with digital platforms. Digital technology also expands access to financial systems for communities previously excluded from conventional banking.

However, despite their significant potential, cryptocurrencies also present challenges and risks. One major challenge is extreme price volatility—cryptocurrency values can shift rapidly,

posing potential losses for inexperienced investors (Yuliana, 2022). Regulatory uncertainty also remains a concern. In Indonesia, digital assets are classified as commodities under BAPPEBTI, not as legal payment instruments, limiting their transactional use.

From an informatics engineering perspective, cybersecurity is a vital component of successful digital asset implementation. (Pratama, 2021) argues that strengthening infrastructure—secure networks, reliable data encryption, and machine-learning-based anomaly detection—is essential to prevent misuse. Collaboration among technology developers, financial institutions, and academia is crucial for building systems that are efficient, regulation-compliant, and trustworthy.

Digital literacy is equally important. Government and educational institutions must actively educate the public about digital assets—how they work, their benefits, and their risks—to ensure informed decision-making and avoid fraudulent schemes. Ultimately, synergy among developers, users, and regulators is essential for building a safe, inclusive, and sustainable digital ecosystem.

Overall, informatics engineering plays a major role in cryptocurrency development, from technological design and cybersecurity to improving financial accessibility (Perayunda & Mahyuni, 2022; Selijusi & Sibarani, 2023). With clear regulations, stronger education, and ongoing technological advancement, digital assets could become an important pillar of Indonesia's economic transformation.

While organizational maturity forms the foundation of sustainable cybersecurity, long-term resilience requires strategic integration between Quality Management Systems (QMS) and enterprise-wide security architectures. QMS enables organizations to align cybersecurity objectives with overall business strategies, ensuring that information security initiatives support operational continuity, customer trust, and competitive advantage. This strategic alignment is particularly important in digital economies, where data integrity and service availability directly influence organizational reputation and financial performance.

A key benefit of QMS-driven cybersecurity is the establishment of a risk-based approach. Rather than applying uniform security controls across all systems, organizations can prioritize assets based on criticality and impact. Through systematic risk assessments, QMS facilitates the identification of high-value information assets and potential threat vectors. This enables targeted investments in security controls, optimizing resource allocation while maximizing risk reduction. Such prioritization is essential in resource-constrained environments, where organizations must balance cybersecurity spending with other operational needs.

Moreover, QMS promotes the standardization of incident management processes. Clearly defined procedures for detection, containment, eradication, and recovery enhance organizational readiness during cyber incidents. Post-incident reviews, mandated under QMS frameworks, provide structured opportunities for learning and improvement. Lessons learned from security breaches are documented and translated into corrective and preventive actions, reinforcing organizational memory and reducing the likelihood of recurring incidents.

The integration of QMS also strengthens business continuity and disaster recovery planning. Cyber incidents increasingly disrupt core operations, from payment systems to supply chains. By embedding cybersecurity considerations into business continuity management, organizations can ensure the rapid restoration of critical services. Regular testing of recovery plans, supported by QMS audit cycles, enhances preparedness and minimizes

downtime. This capability is particularly vital for sectors such as banking, healthcare, and e-government services, where service disruptions can have significant societal impacts.

Another strategic advantage of QMS is its ability to support innovation while managing risk. Digital transformation initiatives, including cloud adoption and remote work arrangements, introduce new vulnerabilities. QMS provides governance mechanisms to evaluate security implications before deploying new technologies. Change management processes ensure that cybersecurity risks are assessed, mitigated, and communicated across stakeholders. This balance between innovation and control enables organizations to pursue digital growth without compromising security.

Human capital development remains central to this transformation. QMS encourages continuous professional development through structured training programs and competency assessments. Cybersecurity roles evolve rapidly, requiring ongoing upskilling in areas such as threat intelligence, incident response, and regulatory compliance. By integrating cybersecurity competencies into performance management systems, organizations can cultivate specialized expertise while fostering a culture of accountability.

In the Indonesian context, workforce capability gaps remain a significant challenge. Many organizations struggle to recruit and retain qualified cybersecurity professionals. QMS can partially address this issue by institutionalizing knowledge through documentation and standardized procedures, reducing reliance on individual expertise. Partnerships with universities and vocational institutions can further support talent development, creating a pipeline of skilled professionals aligned with industry needs.

Additionally, QMS enhances transparency and stakeholder communication. Regular reporting on cybersecurity performance builds trust among customers, regulators, and business partners. Disclosure of security policies and certifications signals organizational commitment to protecting sensitive information. This transparency is increasingly important as consumers become more aware of data privacy and security risks.

From a policy perspective, governments play a pivotal role in promoting QMS-based cybersecurity adoption. Regulatory frameworks can incentivize certification through tax benefits, procurement preferences, or compliance recognition. National cybersecurity strategies can incorporate QMS principles to standardize security practices across public and private sectors. In Indonesia, strengthening coordination between regulatory bodies such as Kominfo and BSSN can accelerate the adoption of integrated quality and security management systems.

Furthermore, international collaboration offers valuable opportunities for knowledge exchange. Participation in global standards organizations and cybersecurity forums enables Indonesian stakeholders to learn from best practices and emerging trends. QMS provides a common language for such collaboration, facilitating interoperability and mutual recognition of certifications.

Economic considerations also underscore the importance of sustainable cybersecurity. Cyber incidents impose significant costs, including system restoration, legal liabilities, and reputational damage. By embedding cybersecurity within QMS, organizations can shift from reactive spending to proactive investment. Preventive controls, continuous monitoring, and employee training collectively reduce the total cost of security over time. This long-term

perspective aligns with sustainable development goals, emphasizing resilience and responsible resource management.

Ethical considerations further enrich the QMS–cybersecurity nexus. Responsible data handling, user privacy protection, and transparency in automated decision-making are increasingly recognized as organizational obligations. QMS supports ethical governance by formalizing policies and accountability structures. As artificial intelligence becomes more prevalent in security operations, ethical frameworks embedded within QMS ensure that technology deployment respects human rights and societal values.

Looking forward, the integration of QMS and cybersecurity will continue to evolve in response to emerging technologies and threat landscapes. Quantum computing may challenge existing cryptographic systems, while artificial intelligence could amplify both defensive and offensive cyber capabilities (Nahdi & Sili, 2022). Organizations equipped with mature QMS frameworks will be better positioned to adapt to these disruptions through structured learning and continuous improvement.

In summary, Quality Management Systems provide a comprehensive framework for embedding cybersecurity into organizational strategy, operations, and culture. Beyond technical safeguards, QMS fosters leadership engagement, workforce development, stakeholder trust, and adaptive governance. For Indonesia and other developing economies, this integrated approach offers a practical pathway to building sustainable digital resilience.

Ultimately, cybersecurity sustainability is not a static achievement but an ongoing journey. Organizations that leverage QMS principles can continuously refine their defenses, anticipate emerging risks, and align security initiatives with broader business and societal objectives. By doing so, they move beyond compliance toward a resilient digital future, where security becomes an enabler of innovation and sustainable growth rather than a constraint.

CONCLUSION

This study confirms that informatics engineering plays a vital role in developing digital assets as alternative solutions during an economic crisis. Through blockchain technology, digital financial systems can operate with transparency, security, and high decentralization, reducing dependence on traditional financial institutions. Cryptographic algorithms and strong cybersecurity measures ensure safe and reliable digital transactions.

Informatics engineering also contributes to infrastructure development, data management, and the implementation of machine learning for detecting potential digital financial threats. With adequate digital literacy and clear government regulations, digital assets such as cryptocurrency, NFTs, and CBDCs can become important instruments in strengthening national economic resilience. Overall, collaboration among academics, technology developers, and financial institutions is key to creating an inclusive, efficient, and sustainable digital asset ecosystem.

REFERENCES

CBDC. (2025). Examining the role of blockchain and public-private partnerships in design and deployment of blockchain-enabled CBDC. *Digital Business*, *5*(1), 100111.

Chairunnas, A., & Sugianto, E. (2024). Teknologi blockchain dalam transformasi keuangan dan perbankan. *Jurnal Ekonomi, Energi, Dan Sistem Sosial*, *5*(2).

https://doi.org/10.62794/je3s.v5i2.3568

Collberg, C., & Davidson, J. (2011). Toward digital asset protection. *IEEE Intelligent Systems*, *26*(6), 8–13.

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation Review*, *2*, 6–10.

Fund, I. M. (2025). *El Salvador: Selected issues*.

Guliyev, B., & Bethlendi, A. (2026). Blockchain vs. centralized ledgers in CBDCs. *Scientific Culture*.

Hidayat, A. (2020). Analisis pengaruh perkembangan cryptocurrency terhadap investasi digital di Indonesia. *Jurnal Ekonomi Dan Bisnis Digital*, *3*(2), 112–120.

Institute, M. (2025). *Global digital asset adoption: Sub-Saharan Africa*.

International. (2025). Bitcoin research in business and economics: A bibliometric and topic modeling review. *Journal of Risk and Financial Management*, *4*(4), 68.

Nahdi, T., & Sili, E. B. (2022). Legalitas penggunaan cryptocurrency sebagai alat investasi jangka panjang di Indonesia. *Commerce Law Journal*, *3*(1). https://doi.org/10.29303/commercelaw.v3i1.2816

Perayunda, I. G. A., & Mahyuni, L. P. (2022). Faktor-faktor yang mempengaruhi keputusan investasi cryptocurrency pada kaum milenial. *Jurnal Manajemen Dan Bisnis*, *6*(3). https://doi.org/10.24034/j25485024.y2022.v6.i3.5224

Pratama, R. (2021). Keamanan sistem blockchain dalam pengembangan aset digital di era industri 4.0. *Jurnal Informatika Dan Teknologi Komputer*, *5*(1), 45–53.

Sari, D., & Rahman, F. (2021). Peranan teknologi blockchain dalam sistem keuangan digital. *Jurnal Teknologi Informasi Dan Komunikasi*, *9*(1), 67–74.

Sari, S. A., & Nasution, M. I. P. (2023). Implementasi teknologi blockchain dalam uang digital. *Jurnal Ilmiah Ekonomi Dan Manajemen*, *2*(12). https://doi.org/10.61722/jiem.v2i12.3124

Selijusi, I. B., & Sibarani, B. B. (2023). Return dan risiko investasi terhadap volume perdagangan cryptocurrency Bitcoin. *Jurnal Bisnis Administrasi Umum*, *9*(1). https://doi.org/10.35968/jbau.v9i1.1168

Shameli-Sendi, A., & Aghababaei-Barzegar, R. (2016). Taxonomy of information security risk assessment (ISRA). *Computers & Security*, *57*, 14–30.

Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution*. Penguin.

Wesselbaum, D. (2020). Cryptocurrency during economic crises. *Journal of Economic Studies*, *47*(5), 1073–1091.

Yermack, D. (2017). Corporate governance and blockchains. *Review of Finance*, *21*(1), 7–31. https://doi.org/10.1093/rof/rfw074

Yuliana, M. (2022). Risiko dan tantangan penggunaan cryptocurrency di Indonesia. *Jurnal Ekonomi Modern*, *6*(3), 201–210.

© 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY SA) license (https://creativecommons.org/licenses/by-sa/4.0/).