Journal of Process Management and New Technologies
Vol. 14, Issue 1-2, 2026, pp. 104-116

SMART CONTRACTS FOR FINANCIAL SECURITY: PROCESS AUTOMATION, RISK MITIGATION, AND ORGANIZATIONAL IMPLICATIONS

Svetlana MARKOVIĆ[1*], Radovan VLADISAVLJEVIĆ[2], Marko MARKOVIĆ[3]

[1]*Faculty of Law for Commerce and Judiciary, Novi Sad, University Business Academy in Novi Sad, Serbia, svetlana.markovic@pravni-fakultet.info*
https://orcid.org/0000-0003-2776-6519

[2]*Faculty of Economics and Engineering Management, Novi Sad, University Business Academy in Novi Sad, Serbia, radovan.vladisavljevic@fimek.edu.rs*
https://orcid.org/0000-0002-8502-8584

[3]*Faculty of Applied Management, Economics and Finance, Belgrade, University Business Academy in Novi Sad, Serbia, marko.markovic@mef.edu.rs*
https://orcid.org/0009-0002-6449-6589

Abstract: *Smart contracts are one of the most prevalent and important blockchain-based technologies in the field of financial security, as the automatic execution of predefined rules provides additional efficiency, lowers costs and minimizes the involvement of intermediaries. This research will examine the use of smart contracts for process automation, risk reduction and organizational restructuring in the financial sector. In particular, the interaction between centralized and decentralized financial systems, the technology behind the implementation of blockchain and security issues associated with the use of smart contracts will be considered. At the same time, escrows will be presented as an example of the practical use of smart contracts for financial operations. The results of this analysis will show that smart contracts can be used as a means to increase the reliability of financial operations; however, their widespread use depends on proper regulation, security assessment and integration with the existing financial infrastructure.*

Keywords: *Smart contracts, blockchain technology, financial security, decentralized finance (DeFi), escrow mechanism*

Original scientific paper
Received: 05.11.2025
Accepted: 12.01.2026
Available online: 14.06.2026
DOI: 10.5937/jpmnt14-68025

* Corresponding author

1. Introduction

The rapid digitalization of financial services has significantly changed the way modern financial institutions operate. On one hand, new opportunities for greater efficiency, automation, and security have emerged, while on the other hand, new challenges in the areas of data protection, risk management, and organizational control have also arisen. At the core of these changes, blockchain technology plays the most significant role through smart contracts, which are a digital form of contracts that execute themselves according to predefined rules implemented in an algorithm that carries out subsequent processing and later distribution of the contracts mentioned via blockchain infrastructure (Kumar et al., 2025).

Since the emergence of Bitcoin as the first form of crypto technology and the subsequent development of blockchain platforms like Ethereum, the financial sector has gained a new solution that executes, verifies, and secures transactions in real time (Javaid et al., 2022). Through this technology, the financial sector can automate its processes, reducing dependence on intermediaries and establishing a new form of trust and accountability in an increasingly interconnected digital economy (Tanchangya et al., 2025).

The very concept of smart contracts represents digital protocols that are automatically executed as soon as predetermined conditions are met. Unlike traditional contracts that rely on human intermediaries, legal institutions, and centralized oversight, smart contracts utilize the immutability and cryptographic protection of blockchain networks to ensure the accuracy and integrity of transactions without the need for a third party. In this way, the room for errors, fraud, and unauthorized modifications of records is reduced, as blockchain protects all transactions and records within its blocks better than human models of cryptography. As noted in the literature, smart contracts contribute to making transactions between participants in the network reliable and verifiable, while simultaneously reducing transaction costs (Bassan & Rabitti, 2024). The application of smart contracts enables a flow that begins with sustainable financing of supply chains, central bank digital currencies, decentralized lending and borrowing, to the automated processing of insurance claims and transaction systems that operate solely based on smart contracts (Hariyani et al., 2025). They also play an important role in decentralized financial systems, known as DeFi, as they automate financial transactions in this environment and allow users to exchange directly between individuals, without traditional intermediaries such as banks or exchange offices (Romero-Castro et al., 2025). Smart contracts become even more useful when they relate to other modern technologies, such as the Internet of Things, artificial intelligence, and cloud computing. Such integration enables real-time monitoring of processes, automatic detection of deviations, and quicker responses to potential risks (Soori et al., 2023). For example, blockchain systems that use smart contracts can define operational rules for IoT devices, record risks that are visible to all contracting parties, and reject state changes if it is assessed that the risk level is too high (Gholami et al., 2025). Risk reduction is another key contribution of smart contracts to financial security. Since transactions recorded on the blockchain cannot be altered afterward, the possibility of data manipulation and financial fraud is significantly reduced (Germanos et al., 2026).

Financial institutions may also face the legal frameworks of the countries in which they operate, as they must precisely align traditional legal and business requirements with decentralized, automated, and blockchain systems. The aim of this paper is to provide a comprehensive analysis of smart contracts as an important instrument of financial security. Attention will be paid to their role in process automation, risk reduction, and the transformation of organizational structures in financial institutions (Said et al., 2025). In the following sections of the paper, the technical foundations of smart contract architecture will be addressed, the ways in which automation contributes to financial security, the risks associated with their application, as well as the broader organizational and managerial implications for the

financial sector. By synthesizing contemporary research in these areas, the paper aims to provide a balanced understanding of the opportunities and limitations of smart contracts in the realm of financial security. In this way, the analysis can be useful not only for researchers but also for practitioners, regulators, and financial institutions that are considering or already applying this technology.

2. Financial system and decentralization

The modern financial system is traditionally organized around centralized institutions that play a key role in maintaining monetary stability, trust, liquidity, and the integrity of transactions. In such an architecture, banks, payment processors, and other financial intermediaries function as interconnected elements of the institutional framework. Their role is not only technical but also regulatory and fiduciary, as they provide the conditions for executing payments, safeguarding funds, managing risk, and protecting users of financial services (Arshadi & Dombrowski, 2026).

Central banks are often viewed in contemporary literature as institutional "third authorities" that enable trust and coordination in conventional finance, in contrast to decentralized financial models that seek to operate without relying on such central intermediaries. Banks and financial intermediaries, on the other hand, represent the operational foundation of the traditional system, but they are also institutions whose role decentralized financial models seek to diminish by enabling more direct financial relationships between users (Preziuso et al., 2023). The centralized financial system is based on the assumption that security arises from institutional responsibility, legal regulation, and administrative control. In this sense, users of financial services do not need to directly verify each transaction or assess the technical validity of the system but rather rely on the institutions that manage transaction flows and records. This model has significant advantages, especially in terms of clear accountability, regulatory compliance, consumer protection, and well-developed procedures for dispute resolution. However, centralization simultaneously creates certain limitations. When control, record-keeping, and management of resources are concentrated in a limited number of institutions or infrastructures, the system's dependence on their proper functioning increases. In the event of a technical failure, abuse of administrative privileges, security breaches, or institutional failure, the consequences can have a broader systemic impact (Soana & De Arruda, 2024; Cappai, 2023).

Recent research shows that centralized financial systems, although stable and institutionally developed, may have certain limitations. They most often relate to high transaction costs, slower settlement processes, lower transparency, and dependence on intermediaries. An additional challenge is the fact that users' funds and key decisions are often under the control of a limited number of institutions, which can increase security and organizational risks. In this context, decentralized finance, or DeFi models, represent an attempt to mitigate some of these weaknesses through more direct transactions between users, lower costs, faster execution, and greater accessibility of financial services (Zheng, 2026). Interest in decentralized financial architectures has further increased due to distrust in certain centralized crypto-financial services, especially following cases of exchange hacking, theft of digital assets, and failures of certain platforms (Jiang et al., 2026).

When comparing the models of centralized and decentralized financial systems, it is important to emphasize the analysis of all aspects related to efficiency, transparency, control, accountability, and resilience. Centralized models provide security in adhering to institutional rules thru specially developed mechanisms that comply with prescribed regulations, but they can limit transparency and increase the consequences of systemic failures. On the other hand,

the decentralized approach contributes to greater confidentiality, availability, and resilience thru a model that controls the validation and control system but requires a new form of flow oversight compared to the centralized approach (Theodorakopoulos et al., 2024). In this context, the decentralized approach does not represent any competitive substitute for the centralized one, but rather its modern reconstruction that incorporates contemporary technologies into its operation. This reduces dependence on central intermediaries and increases transparency, but at the same time requires careful consideration of new risks and accountability mechanisms.

3. Blockchain technologies

Blockchain technology is most associated with a mechanism that enables the recording, storage, and verification of transactions within a network of participants, without relying on a single central database or a unique administrator. Unlike traditional systems that use standard protocols and mechanisms in the processing, blockchain is based on the principle of enabling participants in the network to jointly maintain a consistent version of the data without the need for complete trust in a central authority (Tripathi et al., 2023; Almarri & Aljughaiman, 2024).

The foundation of this technology consists of distributed data storage, cryptographic protection mechanisms, and consensus mechanisms. A series of transactions are grouped into blocks that are interconnected, forming a chain that contains dozens of records of transactions on the network, making it difficult to alter the data later without detection. This ensures integrity, verifiability, traceability, and greater resistance of the records to manipulation. These characteristics are particularly significant in the financial sector, where the accuracy of transaction records, the ability to audit, and trust in the data are of crucial importance (Chen et al., 2024). Blockchain can be used as a system in both public and private models; the public model allows access to all users in the network with a high level of transparency, but it may have limitations regarding privacy and performance.

A private blockchain provides greater access control, while a consortium model allows multiple organizations to jointly manage the network. These models are particularly relevant for financial institutions, which must balance transparency, confidentiality, regulatory requirements, and operational efficiency (Tawfik et al., 2025). It is often associated as the foundation of all cryptocurrencies, but it is actually the infrastructure that enables the strengthening of trust, automation of processes, data management, and verifiable recording of transactions. Its application can contribute to faster settlements, reduced dependence on intermediaries, and greater transparency of financial flows (Almi'ani et al., 2026). However, the application of blockchain faces challenges such as scalability, interoperability, integration with existing financial systems, regulatory compliance, and risk management (Habib et al., 2022). Therefore, blockchain should not be viewed as a standalone solution for all financial security issues, but rather as a technological foundation that can enhance the integrity, transparency, and resilience of the system if properly integrated into a broader institutional and regulatory framework (Quan et al., 2025).

4. Smart contract

Smart contracts represent one of the most significant concepts that changes the way trust is established and digital transactions are executed. At their core, smart contracts represent an algorithm that automatically executes, controls, or documents legally relevant processes in accordance with the conditions that are predefined within the code itself (Bassan & Rabitti, 2024). Their key characteristic lies in the ability to autonomously execute contractual obligations

once certain conditions are met, while the immutability of blockchain records further ensures the integrity and authenticity of transactions. However, it is precisely that immutability that increases the importance of the quality of the code, as errors and vulnerabilities after implementation can lead to lasting and financially significant consequences.

In modern environments, the application of smart contracts goes beyond the realm of cryptocurrencies and encompasses the automation of banking processes, trading activities, fraud prevention systems, identity verification, and other financial services that rely on transparency and cryptographically secured infrastructure of blockchain networks (Ding et al., 2025). Due to the direct management of financial assets and business rules, the security of smart contracts represents one of the most important prerequisites for their broader application, which indicates that security is a strong essential factor and that it is important to keep the system secure and resistant to data manipulation (Marković & Soleša, 2025).

In response to these challenges, various approaches have been developed for security verification, including static and dynamic analysis, symbolic execution, data flow analysis, fuzzing techniques, and formal verification, all aimed at identifying potential vulnerabilities before the implementation of contracts in a production environment. Formal methods and model checking approaches are of particular importance as they enable mathematical verification of a contract's compliance with specified requirements and security demands, thereby increasing the reliability of blockchain systems in financial transactions.

Contemporary practice shows that machine learning is having an increasing impact, as it complements traditional techniques by analyzing a large number of contracts and automatically recognizing patterns associated with known classes of vulnerabilities, including reentrancy attacks, arithmetic errors, unchecked calls, and access control issues (Salzano et al., 2026). The combination of standard methods, automated tools, and machine learning models today represents the dominant approach to ensuring the security of smart contracts in financial systems. In addition to automating business processes, smart contracts play a significant role in enhancing auditing and preserving data integrity, enabling decentralized storage of evidence, automatic validation of information, and transparent recording of all activities without relying on centralized authorities. In this way, they simultaneously represent a mechanism for strengthening trust, improving data management, and increasing the efficiency of financial processes (Soleša et al., 2025). Figure 1 shows the concept on which smart contracts are based and the algorithm execution procedure that implements smart contracts.

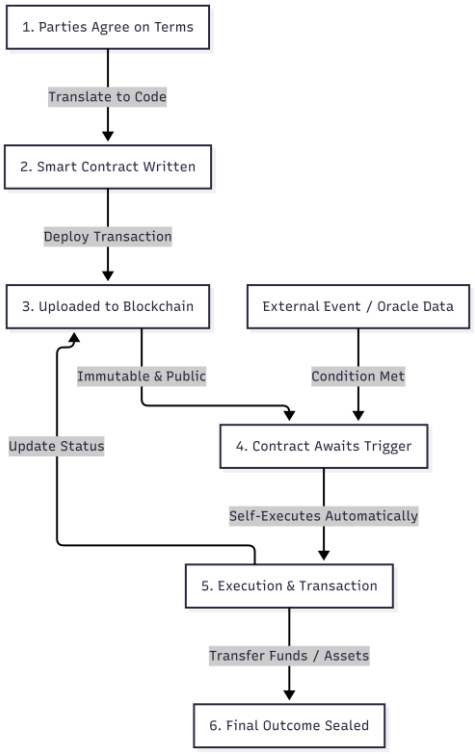

Figure 1. Smart Contract concept
Source: Authors

5. Escrow account

The Escrow mechanism is the best example of how smart contracts can be used to achieve a higher degree of automation while increasing business security. "An escrow account consists of funds held by a third party, who collects, holds, and disburses the funds pursuant to a contract or an obligation between two parties" (Mills, 1994). "It is essentially a deposit of documents, securities, goods or money in a neutral and impartial party with specific instructions on how, in what way, and to whom the escrow holder hands over the documents, goods or money" (Handayani et al., 2021). Risks related to business are an integral part of everyday life, for this reason an escrow mechanism was formed that should protect the contracted parties, unfortunately this includes the mediation of a third party. The escrow mechanism is most often used during trade, the buyer would contract for the goods, provide funds in a special escrow account, usually with a bank, the seller would send the goods and collect the same after the goods are delivered to the buyer.

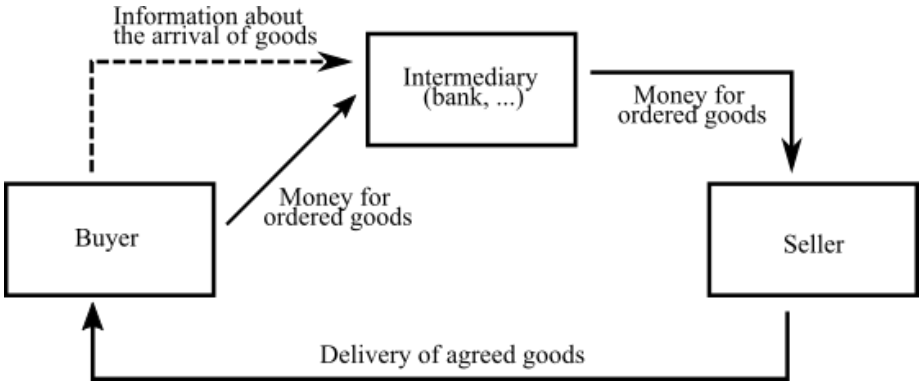

Figure 2. Schematic of the Escrow mechanism
Source: Authors

The basic idea of the Escrow mechanism can be seen in the previous image. When the sale of some goods is contracted, the buyer secures the means of payment for the ordered goods through an intermediary. These funds are only presented to the seller, in order for the seller to get the funds, the goods must be delivered to the buyer. Funds are sent to the seller only after sending the information about taking over the goods.

This type of mechanism increases security in business, however, in order for the escrow mechanism to function, it is necessary to have an intermediary in the form of a bank or an agent who will take care of keeping the money and later processing requests for payment or refund. This brokerage has two major drawbacks, the first is the costs generated by employing an intermediary, the second drawback is related to the very nature of the mechanism that requires the buyer to capture their funds before the contracted goods arrive.

The use of blockchain technology and smart contracts can solve the first problem completely, the second problem can only be partially solved. Smart contracts are a part of blockchain technology and are a piece of code that allows the execution of predetermined and agreed upon actions when the necessary conditions are met. On the example of the Escrow mechanism, the payment of funds is executed when a certain customer receives the goods. In order not to trap the funds, the mechanism can be set so that the funds are returned to the customer after a certain period of time.

This decision-making process can be represented through a simple pseudocode example that demonstrates the two possible outcomes of the escrow mechanism: releasing the funds to the seller after delivery confirmation or refunding the buyer if the agreed deadline has passed.

Pseudocode 1. Smart Contract-Based Escrow Procedure

```
1. if (delivery_confirmed == true)
2. {
3.   transfer_funds_to_seller();
4. }
5. else if (deadline_passed == true)
6. {
7.    refund_buyer();
8. }
```

A smart contract does not generate costs or is subject to changes in business policy, so the first problem related to costs is completely solved. Another problem related to tying up the customer's funds before the delivery of the goods cannot be solved using smart contracts, the only thing that can be done is to process the payment as quickly as possible. The classic escrow

mechanism relies on people being part of the partnership. This means that banks or agencies dealing with escrow accounts have working hours, non-working days and the like. The smart contract on the other hand is available continuously every day.

Table 1. Characteristics of classic escrow and the death of the contact escrow account

Characteristic	Traditional escrow	Smart contract escrow
Mediator	bank or institution	code
Costs	high	low
Speed	slow process	automatic execution
Transparency	limited	complete on blockchain
Risk of manipulation	possible	minimal

Source: Authors

From the previous table, it is possible to see in a clear and systematic way the characteristics of the classical escrow and death contract escrow accounts. Features that we have not taken into account so far are transparency and the risk of manipulation. The classic escrow account mechanism is based on banks or financial institutions that have limited transparency at best. Blockchain technologies are public and available to everyone, so transparency is complete and not only to the participants in the business venture. Another characteristic is related to the risk of manipulation. Despite the robust banking system, clearly defined and codified rules, manipulation with escrow accounts is possible. With the use of smart cotract escrow accounts, manipulation is theoretically possible, but the nature of decentralized financial mechanisms with the use of blockchain technologies makes manipulation practically impossible.

Blockchain functions as a decentralized and distributed ledger of transactions where there is no central governing body. Transactions are recorded on a large number of nodes in the network, where each node can own a copy of the entire blockchain. Adding new blocks is done through a consensus mechanism that achieves network agreement on the validity of transactions and the integrity of the new block. To further illustrate the practical implementation of an escrow mechanism based on smart contracts, a simplified example written in Solidity is presented below in Algorithm 1, which demonstrates the core structure and execution logic of a smart contract-based escrow system.

Algorithm 1. Solidity Implementation of a Smart Contract-Based Escrow Mechanism

```
1. //SPDX-License-Identifier: MIT
2. pragma solidity ^0.8.0;

3. contract Escrow {

4.    address public buyer;
5.    address payable public seller;
6.    address public arbiter;

7.    bool public isApproved;

8.    constructor(address payable _seller, address _arbiter) payable {
9.       buyer = msg.sender;
10.      seller = _seller;
11.      arbiter = _arbiter;
12.   }
```

```
13.  function approve() public {
14.    require(msg.sender == buyer || msg.sender == arbiter, "Not authorized");
15.    require(!isApproved, "Already approved");

16.    isApproved = true;
17.    seller.transfer(address(this).balance);
18.  }

19.  function getBalance() public view returns(uint) {
20.     return address(this).balance;
21.  }
22. }
```

A smart contract does not generate costs or is subject to changes in business policy, so the first problem related to costs is completely solved. Another problem related to tying up the customer's funds before the delivery of the goods cannot be solved using smart contracts, the only thing that can be done is to process the payment as quickly as possible. The classic escrow mechanism relies on people being part of the partnership. This means that banks or agencies dealing with escrow accounts have working hours, non-working days and the like. The smart contract on the other hand is available continuously every day.

Table 2. Roles in the escrow mechanism

Role	Function
buyer	deposit of funds
smart contract	saves funds
arbitrator	resolves the dispute
seller	receives funds

Source: Author's

From the code, it can be seen that the participants in this example, in addition to the buyers and the seller, are also the arbitrator as well as the smart contract itself. An arbitrator is important so that funds are not "trapped" due to some unforeseen circumstances. The smart contract is linked to the blockchain, the blockchain is just a system for storing data in a special way and as such can be considered as an independent entity. Cryptocurrencies are closely related to blockchain technologies, they cannot exist without blockchain. It follows that cryptocurrency payments according to the model presented in the previous segment are significantly facilitated and can be fully automated.

```
constructor(address payable _seller, address _arbiter) payable
```

The preceding constructor forms a new contract, defines participants, and sends assets to the contract. This line of code forms the skeleton of the contract and defines the individual details.

```
address(this).balance
```

This piece of code "locks" the funds into the contract, so that the funds are neither with the buyer nor with the seller. This is perhaps the most specific part of the code because reserved funds are visible online, not available to anyone until the business venture is closed.

```
seller.transfer(address(this).balance);
```

The buyer or arbitrator confirms the transaction, and the funds are "released" to the seller. In this code segment, the smart contract reaches the end of its usefulness. The arbitrator is important and represents a third, neutral party who is trusted by both parties in the business venture. This role is important because there is a potential danger of permanently locking up funds. It must not be forgotten that the smart contract is only a part of the code, this form has nothing to do with the legal form of the contract, nor is there a single point of regulation of the contract, nor a body that would make an appropriate solution due to a dispute.

The code shown is still a relatively crude example of an escrow mechanism model. For real use, it is necessary to define additional elements. For example, the displayed code lacks a timeout, which would automatically trigger some desired action, such as a refund, after the time has expired. The refund itself must also be defined, whether there are any penalties for failure to execute a business venture and similar details. Multisignature authorization is vital because multiple confirmations drastically reduce the possibility of manipulation. Then it is necessary to have some form of connection to the "real" world, for this it is best to use Oracle delivery verification. Oracle systems allow smart contracts to access data from the external environment. In the context of escrow transactions, oracle can transfer information about the delivery of goods from the logistics system, which enables the automatic execution of contracts and the release of funds after confirmation of delivery. Also, it is possible to form communication between different blockchain chains. "Cross-chain communication represents a fundamental paradigm shift within the blockchain ecosystem, enabling disparate blockchain networks to interact and share information seamlessly" (Ray, 2024).

6. Conclusion

Although they are yet another technology based on blockchain, smart contracts have managed to offer a new model and innovation in the world of finance. With their capabilities, they offer great potential and changes in the methods of conducting transactions and other business processes. Given that they enable automatic execution of all the conditions of an agreement in a way that increases efficiency, reduces operational costs, processes transactions more quickly, and decreases the need for intermediaries or individuals who would have to verify, they represent a mechanism that more and more companies are using in their operations. All of this leads to an increase in transparency and reliability of operations within financial systems. This paper explores the role of smart contracts in the business environment, with a focus on their foundation, namely blockchain technology, and areas of application such as decentralized financial systems. Smart contracts reduce the risk of fraud and errors in the process of conducting financial transactions; thus, the use of smart contracts in combination with other modern innovations, such as artificial intelligence, the Internet of Things, and cloud computing, offers an even greater range of potential applications and enables the development of better tools for risk management and process control. A practical example of the escrow mechanism illustrates how smart contracts can successfully automate contractual obligations and enhance transaction security while reducing costs associated with independent intermediaries. However, the analysis also shows that technical vulnerabilities, coding errors, and the lack of adequate legal frameworks remain significant limitations that can hinder broader adoption. Therefore, ensuring the security of smart contracts through auditing, formal verification, and continuous monitoring is a key prerequisite for their successful implementation. Smart contracts are a powerful tool that can enhance financial security and modernize services, but with the caveat that their development requires significant support

from regulatory frameworks, the ability of organizations to integrate this solution into their systems, as well as technological readiness. As digital transformation continues to redefine the global economy, smart contracts are expected to play an increasingly important role in creating safer, more transparent, and more efficient financial ecosystems.

References

Almarri, S., & Aljughaiman, A. (2024). Blockchain Technology for IoT Security and Trust: A Comprehensive SLR. Sustainability, 16(23), 10177. https://doi.org/10.3390/su162310177

Almi'ani, K., Mirza, S. B., Siyam, N., Al-Jaziri, S. A., Alqaryouti, O., & Zufferey, C. (2026). Global adoption and impact of blockchain technology in Government: Enhancing transparency, efficiency, and trust in public services. Information, 17(3), 235. https://doi.org/10.3390/info17030235

Arshadi, N., & Dombrowski, T. (2026). Applications and management of blockchain technologies in financial services. Journal of Risk and Financial Management, 19(3), 224. https://doi.org/10.3390/jrfm19030224

Bassan, F., & Rabitti, M. (2024). From smart legal contracts to contracts on blockchain: An empirical investigation. Computer Law & Security Review, 55, 106035. https://doi.org/10.1016/j.clsr.2024.106035

Cappai, M. (2023). The role of private and public regulation in the case study of crypto-assets: The Italian move towards participatory regulation. Computer Law & Security Review, 49, 105831. https://doi.org/10.1016/j.clsr.2023.105831

Chen, H., Wei, N., Wang, L., Mobarak, W., Albahar, M. A., & Shaikh, Z. A. (2024). The Role of Blockchain in Finance Beyond Cryptocurrency: Trust, Data Management, and Automation. Ieee Access, 12, 64861–64885. https://doi.org/10.1109/access.2024.3395918

Ding, H., Li, Q., Wang, C., Ren, H., Li, J., Piao, X., Song, H., & Ji, Z. (2025). How Far Should We Go Away from Smart Contract to Smarter Contractor? A Systematic Review. Blockchain Research and Applications, 100402. https://doi.org/10.1016/j.bcra.2025.100402

Germanos, G., Lekidis, A., Brotsis, S., & Kolokotronis, N. (2026). Blockchain architectures for enhancing EV infrastructure security: A unified framework for addressing sophisticated cyber-attacks. Future Generation Computer Systems, 182, 108426. https://doi.org/10.1016/j.future.2026.108426

Gholami, M., Ghaffari, A., Derakhshanfard, N., Ibrahimoğlu, N., & Kazem, A. a. P. (2025). Blockchain integration in IoT: applications, opportunities, and challenges. Computers, Materials & Continua/Computers, Materials & Continua (Print), 83(2), 1561–1605. https://doi.org/10.32604/cmc.2025.063304

Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S., & Ishfaq, M. (2022). Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing. Future Internet, 14(11), 341. https://doi.org/10.3390/fi14110341

Handayani, O., Sulistiyono, A., & Muryanto, Y. T. (2021). Mandatory escrow account as a manifestation of good faith in peer-to-peer lending. Natural Volatiles & Essential Oils, 8(4), 13290–13300. https://www.nveo.org/index.php/journal/article/view/2854

Hariyani, D., Hariyani, P., Mishra, S., & Sharma, M. K. (2025). A literature review on transformative impacts of blockchain technology on manufacturing management and industrial engineering practices. Green Technologies and Sustainability, 3(3), 100169. https://doi.org/10.1016/j.grets.2025.100169

Javaid, M., Haleem, A., Singh, R. P., Suman, R., & Khan, S. (2022). A review of Blockchain Technology applications for financial services. BenchCouncil Transactions on

Benchmarks Standards and Evaluations, 2(3), 100073. https://doi.org/10.1016/j.tbench.2022.100073

Jiang, S., You, W., Xuan, S., & Shen, J. (2026). Decentralized finance security: A survey of attacks, defenses, and open challenges. High-Confidence Computing, 6(2), 100383. https://doi.org/10.1016/j.hcc.2026.100383

Kumar, R., Sharma, S. K., Kishor, K., & Devi, P. (2025). Decentralized finance evolution: A comprehensive bibliometric analysis. Sustainable Futures, 10, 101209. https://doi.org/10.1016/j.sftr.2025.101209

Marković, M., & Soleša, D. (2025). Security and Data Protection in Artificial Intelligence. Journal of Process Management and New Technologies, 13(1-2), 113–123. https://doi.org/10.5937/jpmnt13-58872

Mills, E. S. (1994). The functioning and regulation of escrow accounts. Housing Policy Debate, 5(2), 203–218. https://doi.org/10.1080/10511482.1994.9521160

Modi, R. (2022). Solidity Programming Essentials - Second edition. O'Reilly Online Learning. https://www.oreilly.com/library/view/solidity-programming-essentials/9781803231181/

Preziuso, M., Koefer, F., & Ehrenhard, M. (2023). Open banking and inclusive finance in the European Union: perspectives from the Dutch stakeholder ecosystem. Financial Innovation, 9(1). https://doi.org/10.1186/s40854-023-00522-1

Quan, J., Duan, Y., & Fu, Q. (2025). Optimizing international trade settlement systems through blockchain-driven tri-chain collaboration: A study on efficiency, costs, and risk mitigation. Sustainable Futures, 10, 101304. https://doi.org/10.1016/j.sftr.2025.101304

Ray, D. (2024). How to Develop Cross-Chain Airdrop dApp: Hands-On Tutorial with Solidity, Next.js & Axelar. Independently published.

Romero-Castro, N., López-Cabarcos, M. Á., Vittori-Romero, V., & Piñeiro-Chousa, J. (2025). Decentralized Finance in Business and Economics Research: A Bibliometric analysis. International Journal of Financial Studies, 13(4), 211. https://doi.org/10.3390/ijfs13040211

Said, Y., Khaddar, A. M., Hassine, L., Eddaoui, A., & Chafiq, T. (2025). The impact of blockchain on the banking sector: A systematic review of applications, challenges, and future directions. Asia and the Global Economy, 6(1), 100133. https://doi.org/10.1016/j.aglobe.2025.100133

Salzano, F., Antenucci, C. K., Scalabrino, S., Rosa, G., Oliveto, R., & Pareschi, R. (2026). An empirical analysis of vulnerability detection tools for solidity smart contracts. Empirical Software Engineering, 31(5). https://doi.org/10.1007/s10664-026-10867-7

Soana, G., & De Arruda, T. (2024). Central Bank Digital Currencies and financial integrity: finding a new trade-off between privacy and traceability within a changing financial architecture. Journal of Banking Regulation, 25(4), 467–486. https://doi.org/10.1057/s41261- 024-00241-2

Soleša, D., Vladisavljević, R., & Marković, S. (2025). The use of smart contracts to preserve the integrity of cold supply chains. In XXI International May Conference on Strategic Management – IMCSM25 Proceedings. pp. 297–306. University of Belgrade, Technical Faculty in Bor. https://doi.org/10.5937/IMCSM25297S

Soori, M., Dastres, R., & Arezoo, B. (2023). AI-powered blockchain technology in industry 4.0, a review. Journal of Economy and Technology, 1, 222–241. https://doi.org/10.1016/j.ject.2024.01.001

Tanchangya, T., Tafsirun, U., Islam, M. S., Islam, N., Chakma, J., & Esquivias, M. A. (2025). Role of financial technology in small-scale natural Resource management through sustainable financing in Venezuela. Social Sciences & Humanities Open, 11, 101636. https://doi.org/10.1016/j.ssaho.2025.101636

Tawfik, A. M., Al-Ahwal, A., Eldien, A. S. T., & Zayed, H. H. (2025). Blockchain-based access control and privacy preservation in healthcare: a comprehensive survey. Cluster Computing, 28(8). https://doi.org/10.1007/s10586-025-05308-x

Theodorakopoulos, L., Theodoropoulou, A., & Halkiopoulos, C. (2024). Enhancing Decentralized Decision-Making with Big Data and Blockchain Technology: A Comprehensive Review. Applied Sciences, 14(16), 7007. https://doi.org/10.3390/app14167007

Tripathi, G., Ahad, M. A., & Casalino, G. (2023). A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges. Decision Analytics Journal, 9, 100344. https://doi.org/10.1016/j.dajour.2023.100344

Zheng, B. (2026). Integrating blockchain technology with financial systems to enhance transparency and efficiency. Kuwait Journal of Science, 53(3), 100613. https://doi.org/10.1016/j.kjs.2026.100613