PD.TVZ.HR
POLYTECHNIC & DESIGN Vol. 14, No. 1, 2026.
Mrežna inačica: ISSN 2459-6302
Tiskana inačica: ISSN 1849-1995
DOI: 10.19279/TVZ.PD.2026-14-1-14

ULOGA PAMETNIH UGOVORA U IZGRADNJI NOVIH DIGITALNIH USLUGA

THE ROLE OF SMART CONTRACTS IN BUILDING NEW DIGITAL SERVICES

Aleksandar Stojanović[1], Željko Kovačević[1], Maja Dabčević[2]

[1] *Zagreb University of Applied Sciences, Vrbik 8, 10000 Zagreb, Croatia*
[2] *Zagreb University of Applied Sciences, Vrbik 8, 10000 Zagreb, Croatia, Student*

SAŽETAK

Pametni ugovori, kao samostalno izvršavajući programi postavljeni na blockchain infrastrukturama, predstavljaju veliki korak naprijed u evoluciji digitalnih usluga. Ugradnjom pravila i procesa izravno u kôd, oni omogućuju automatizaciju, transparentnost i minimiziranje ovisnosti o centralnom autoritetu, čime se smanjuje ovisnost o posrednicima i poboljšava učinkovitost. Ovaj članak pruža pregled tehničkih temelja i arhitekture pametnih ugovora, njihove uloge kao pokretača inovacija digitalnih usluga i njihove primjene u područjima kao što su decentralizirane financije, upravljanje lancem opskrbe, zdravstvo, digitalni identitet i javna uprava. Analiza također ističe ključne izazove, uključujući skalabilnost, sigurnosne ranjivosti, pravnu provedivost, interoperabilnost i socioekonomske prepreke. Konačno, rad razmatra buduće smjerove, s naglaskom na integraciju s novim tehnologijama kao što su umjetna inteligencija i IoT, interoperabilnost među lancima, regulatorni razvoj i decentralizirani modeli upravljanja. U zaključku se sugerira da, iako se pametni ugovori suočavaju s određenim ograničenjima, njihova kontinuirana evolucija pozicionira ih kao kritičnu infrastrukturu za sljedeću generaciju sigurnih, učinkovitih i uključivih digitalnih usluga.

Ključne riječi: *pametni ugovori; blockchain; decentralizirane financije (DeFi); digitalne usluge; interoperabilnost; upravljanje; automatizacija*

ABSTRACT

Smart contracts, as self-executing programs deployed on blockchain infrastructures, represent a major step forward in the evolution of digital services. By embedding rules and processes directly into code, they enable automation, transparency, and central authority dependency minimization, thereby reducing reliance on intermediaries and improving efficiency. This article provides an overview of the technical foundations and architecture of smart contracts, their role as enablers of digital service innovation, and their application across domains such as decentralized finance, supply chain management, healthcare, digital identity, and public administration. The analysis also highlights key challenges, including scalability, security vulnerabilities, legal enforceability, interoperability, and socioeconomic barriers. Finally, the paper considers future directions, emphasizing integration with emerging technologies such as AI and IoT, crosschain interoperability, regulatory development, and decentralized governance models. The findings suggest that while smart contracts face specific limitations, their continued evolution positions them as critical infrastructures for the next generation of secure, efficient, and inclusive digital services.

Keywords: *smart contracts; blockchain; decentralized finance (DeFi); digital services; interoperability; governance; automation*

1. UVOD
1. INTRODUCTION

The ongoing expansion of the digital economy has underscored the need for reliable, efficient, and scalable mechanisms to support service delivery in sectors such as finance, healthcare, logistics, and public administration. Traditional approaches to digital services are largely based on centralised infrastructures, where intermediaries such as financial institutions, public notaries, and regulatory bodies play a crucial role in verifying transactions and executing contracts. Although effective in many respects, these intermediary-dependent models introduce inefficiencies, higher operational costs, and institutional bias [1].

The advent of blockchain technology has provided a new infrastructure for designing decentralised systems, shifting the responsibility for validation and execution from institutions to distributed automatic consensus mechanisms [2]. In this context, smart contracts have emerged as a key innovation. Smart contracts are typically defined as self-executing programmes stored on the blockchain that automatically enforce predefined rules and agreements among participants once specified conditions are met. Their attributes – immutability, transparency, and programmability – enable the automation of contractual or other logic without external oversight, facilitating new models of digital interaction and service delivery [3].

The significance of smart contracts goes beyond their technical architecture, as they represent a shift in how digital services are conceptualised and delivered. By embedding logic and execution directly into distributed infrastructures, smart contracts reduce reliance on third parties, enhance auditability, and potentially lower costs [4]. New applications demonstrate their versatility: from decentralised finance (DeFi) platforms offering lending and trading without banks, to supply chain solutions that automate origin tracking, to public administration systems piloting blockchain-enabled voting and registries. These examples highlight the growing role of smart contracts in reshaping service ecosystems [5].

This paper examines the role of smart contracts in the development of new digital services, focusing on their technical characteristics and socio-technical implications. Specifically, the study addresses the following questions:

1. Which functional properties of smart contracts make them suitable for innovations in digital services?
2. How are smart contracts currently applied in various service domains?
3. What challenges must be addressed for broader adoption?

By analysing these dimensions, the paper aims to contribute to the scientific discourse at the intersection of blockchain technologies and information systems, highlighting smart contracts as both a technical artefact and a socio-economic driver of new digital services.

2. METODOLOGIJA ISTRAŽIVANJA
2. RESEARCH METHODOLOGY

This paper presents a qualitative analysis of secondary sources from scientific and professional literature, as well as technical documentation from leading blockchain platforms. Sources were selected based on relevance, citation frequency, and temporal recency (2016–2024). The analysis was conducted in three steps:

1. identification of the technical and conceptual aspects of smart contracts,
2. review of real-world applications and supporting platforms, and
3. synthesis of challenges and future trends in the context of digital services.

This approach connects theoretical frameworks with practical examples and ensures methodological transparency in addressing the topic.

3. POZADINA I OSNOVE
3. BACKGROUND AND FOUNDATIONS

The development of digital services has historically relied on centralised infrastructures, where organisations implement platforms that mediate access, manage data, and enforce contractual or business rules. Early models of e-commerce and online banking, for example, depended on trusted institutions that

guaranteed the integrity of transactions and provided mechanisms for dispute resolution. Although these services expanded globally, their centralised nature created structural challenges, including increased transaction costs, reliance on institutional trust, and vulnerability to cyberattacks and systemic outages [6].

With the rise of distributed computing and peer-to-peer systems in the early 2000s, researchers began exploring alternatives to centralised service provision. However, these systems often lacked robust mechanisms for enforcing trust and agreements among participants who did not know or trust one another. Blockchain technology, introduced with Bitcoin in 2008 [2], addressed this challenge by introducing a decentralised, cryptographically secured ledger of transactions maintained through consensus protocols. This innovation enabled transactions to be executed without reliance on a central authority, establishing the foundation for the next generation of digital services.

3.1 BLOCKCHAIN KAO TEMELJNA TEHNOLOGIJA

3.1 BLOCKCHAIN AS THE FOUNDATIONAL TECHNOLOGY

Blockchain can be described as a distributed database in which data can only be appended, with transactions grouped into blocks and secured by cryptographic algorithms [7]. Consensus mechanisms such as Proof of Work (PoW) and Proof of Stake (PoS) ensure the validity and ordering of transactions across distributed nodes [8]. These properties – immutability, transparency, and resistance to unauthorised modification – make blockchain networks particularly suitable for enforcing rules in untrusted environments.

The design of blockchain systems also enables programmability, making them more than simple ledgers of financial transactions. Platforms such as Ethereum [9] have expanded blockchain functionality by introducing scripting languages capable of executing smart contracts. This general-purpose programmability has transformed blockchain networks into infrastructure for decentralised applications (DApps), enabling use cases beyond digital currency, including supply chain management, healthcare data sharing, and governance systems [10].

3.2 KONCEPT I KARAKTERISTIKE PAMETNIH UGOVORA

3.2 CONCEPT AND CHARACTERISTICS OF SMART CONTRACTS

The concept of smart contracts predates the invention of blockchain. First articulated by Nick Szabo in the 1990s, smart contracts were described as digital protocols capable of formalising and enforcing contractual relationships through computer code [11]. However, the lack of suitable infrastructure for secure execution limited their practical application. Blockchain technology addressed this issue by providing a decentralised, tamper-resistant environment in which contractual logic can be executed transparently and deterministically.

Smart contracts have several defining characteristics:

- Autonomy: They execute automatically without external intervention.
- Transparency: Their code and execution are visible on the blockchain, allowing for auditability.
- Immutability: Once deployed on a blockchain, they are unchangeable, ensuring predictable behaviour.
- Trust minimisation: They eliminate the need for third parties by embedding rules directly into software.

These properties enable smart contracts to serve as the foundation for digital services that require reliability, efficiency, and the ability to operate within distributed ecosystems.

4. GRAĐA PAMETNIH UGOVORA

4. ARCHITECTURE OF SMART CONTRACTS

At its core, a smart contract is a computer program deployed and executed within a blockchain environment such as Ethereum [3]. A smart

contract typically comprises three key components: contract code, state variables, and transaction triggers. The contract code defines the contract's logic, the state variables store persistent data, and the triggers (such as external inputs or blockchain events) initiate execution. When a transaction invokes a contract function, the blockchain deterministically executes the code across all participating nodes, ensuring a shared and immutable outcome (Figure 1). Listing 1 provides an example of a smart contract for the Ethereum blockchain written in the Solidity language, featuring three functions: deposit, withdraw, and getState. The transaction specifies which of these functions should be triggered during execution.

Execution is guaranteed by the distributed virtual machine embedded in the blockchain platform. Ethereum, for example, relies on the Ethereum Virtual Machine (EVM), which processes bytecode instructions derived from high-level contract languages such as Solidity. Other platforms provide alternative virtual machines and programming models but follow the same general principle of consensus-based distributed execution.

Ispis 1 *Primjer pametnog ugovora za Ethereum pisanog u jeziku Solidity.*

Figure 1 *An example of a smart contract for Ethereum written in Solidity language.*

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

contract SimpleBank {
   // varijabla stanja u kojoj se čuvaju iznosi za svaki račun
   mapping(address => uint256) private balances;

   // događaj za generiranje logova deponiranja
   event Deposit(address indexed user, uint256 amount);

   // događaj za generiranje logova isplata
   event Withdrawal(address indexed user, uint256 amount);

   // funkcija za deponiranje Etera u ovaj pametni ugovor
   function deposit() public payable {
       require(msg.value > 0, "Iznos mora biti veći od 0");
       balances[msg.sender] += msg.value;
       emit Deposit(msg.sender, msg.value);
   }

   // funkcija za isplatu Etera iz ovog pametnog ugovora
   function withdraw(uint256 amount) public {
       require(amount > 0, "Iznos mora biti veći od 0");
       require(balances[msg.sender] >= amount, "Nedovoljan saldo");
       balances[msg.sender] -= amount;
       payable(msg.sender).transfer(amount);
       emit Withdrawal(msg.sender, amount);
   }

   // funkcija za provjeru salda za račun za koji se ona poziva
   function getBalance() public view returns (uint256) {
       return balances[msg.sender];
   }
}
```

4.1 ŽIVOTNI CIKLUS PAMETNOG UGOVORA

4.1 LIFECYCLE OF A SMART CONTRACT

The lifecycle of a smart contract begins with development, during which the contract logic is encoded using platform-specific languages. This is followed by deployment, where the compiled bytecode is sent to the blockchain as a transaction. Once validated and included in a block, the smart contract receives a unique address on the blockchain, making it accessible to participants.

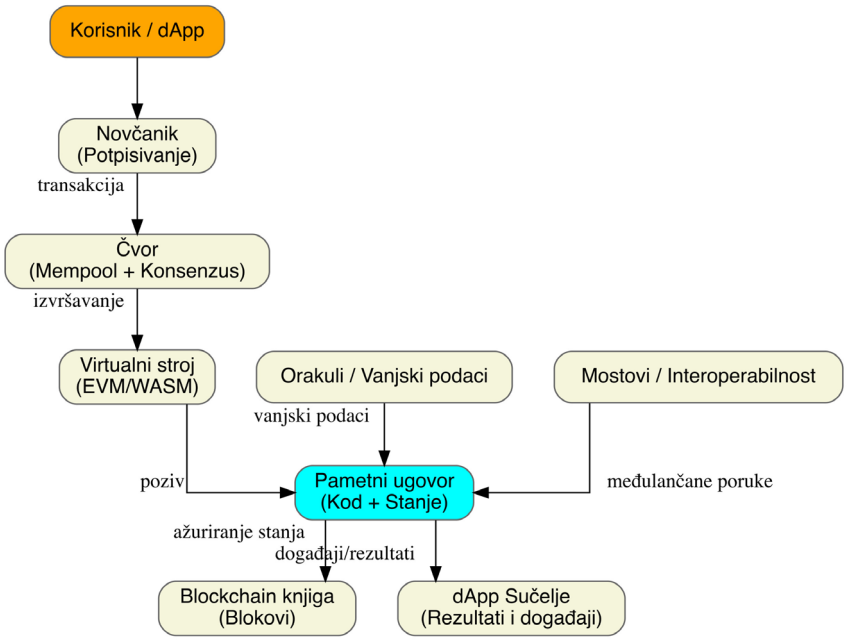
Subsequent interactions with the contract occur through transactions that invoke its functions. These transactions may read or modify the contract's state, depending on the encoded logic. The deterministic nature of blockchain consensus ensures that all participating nodes produce the same execution path and results, eliminating ambiguity or conflicting outcomes. However, this also introduces computational constraints, as complex or resource-intensive operations may be impractical within the fee models used by blockchain systems.

4.2 SIGURNOST I POUZDANOST PAMETNIH UGOVORA

4.2 SECURITY AND RELIABILITY OF SMART CONTRACTS

Smart contracts, despite their potential, pose significant security challenges. Their immutability, while ensuring predictable execution, also means that coding errors or vulnerabilities cannot be corrected once a contract is deployed to the blockchain. High-profile incidents, such as the 2016 attack on Ethereum [12], have shown how flaws in contract logic can lead to substantial financial losses and undermine trust in the ecosystem.

To address these risks, best practices in smart contract engineering emphasise formal verification, code audits, and the use of standardised contract libraries to reduce the likelihood of errors. In addition, research into upgradable contract architectures and governance frameworks aims to balance immutability with controlled adaptability, allowing limited contract modification under predefined conditions.



Slika 1 *Arhitektura decentraliziranog blockchain sustava s pametnim ugovorima.*

Figure 1 *Architecture of a decentralized blockchain system with smart contracts.*

4.3 PRIMJERI PLATFORMI I IMPLEMENTACIJSKIH PRISTUPA

4.3 EXAMPLES OF PLATFORMS AND IMPLEMENTATION APPROACHES

Smart contracts are currently implemented on various blockchain platforms that differ in architecture, programming language, consensus mechanism, and permission model. Ethereum is the most widespread platform and was the first to introduce a general-purpose smart contract model based on the Ethereum Virtual Machine (EVM) and the Solidity language. It uses a Proof of Stake (PoS) consensus mechanism and a gas-based fee model for execution, which together ensure decentralised and deterministic contract execution.

Hyperledger Fabric [13], developed under the Linux Foundation, provides an alternative in the form of a permissioned network that supports defined participant roles and private data channels. Its contracts, known as Chaincode, are written in languages such as Go and Java, facilitating integration with existing enterprise systems.

Cardano [14] offers an approach grounded in formal verification methods, thereby increasing code security and verifiability. Contracts are written in the Plutus language, derived from Haskell, and executed in a controlled environment that reduces the risk of errors.

Platforms such as Solana [15] and Polkadot [16] emphasise scalability and interoperability. Solana supports high throughput and uses Rust, while Polkadot connects multiple chains (parachains) into a single interoperable ecosystem. These approaches illustrate the diversity of smart contract implementations and show that the choice of platform significantly affects the performance, security, and applicability of digital services.

5. PAMETNI UGOVORI KAO TEMELJI DIGITALNIH USLUGA

5. SMART CONTRACTS AS FOUNDATION OF DIGITAL SERVICES

Smart contracts enable digital services by embedding business rules directly into code, allowing automatic execution without intermediaries. This automation increases efficiency, reduces errors, and lowers costs. They also provide transparency, as their logic and outcomes can be publicly verified, which strengthens trust in areas such as finance and supply chains.

By removing the need for trusted third parties, smart contracts expand access to financial and other services. They are further integrated with external data sources through oracles, linking

blockchain systems with real-world events. This makes them particularly relevant for data-driven sectors such as logistics, insurance, and finance.

Smart contracts are now used across multiple domains, offering automation, transparency, and trustless execution.

Financial services and DeFi have seen the earliest adoption, with lending platforms (e.g., MakerDAO, Compound) and decentralised exchanges (e.g., Uniswap) replacing intermediaries, although risks related to security and volatility remain [17]. Figure 2 shows an example of decentralised lending using smart contracts.

In supply chain management, contracts automate payments, delivery verification, and provenance tracking, particularly in sensitive industries such as food, pharmaceuticals, and luxury goods [18].

In healthcare, they manage patient consent, access to medical data, and insurance claims, while also raising regulatory and privacy challenges [19].

Digital identity applications support identity by embedding credentials into blockchain networks, enhancing privacy and cross-border authentication [20].

Finally, governments are exploring smart contracts for voting, land registries, and social benefits, with the potential to increase efficiency but also with concerns regarding governance and inclusiveness [21].

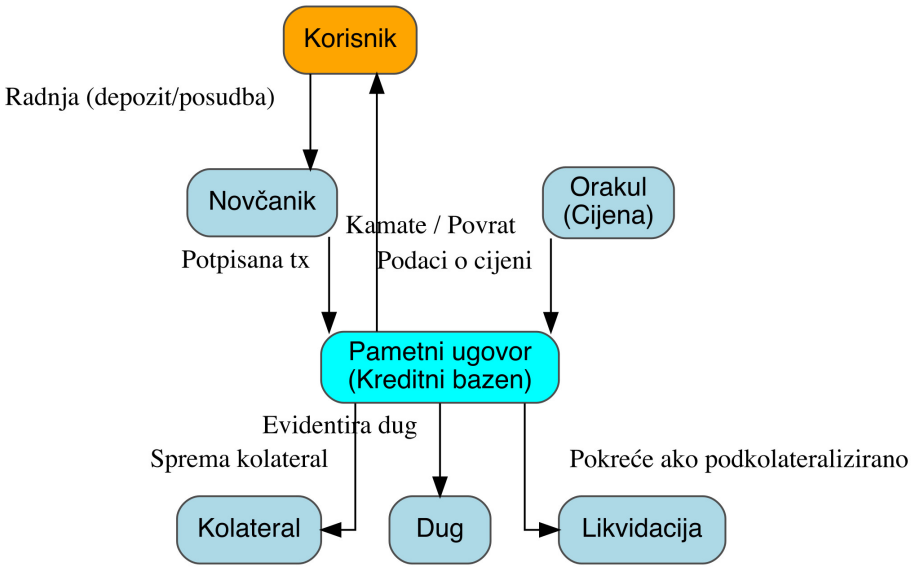
5.1 STUDIJI SLUČAJA UPOTREBE PAMETNIH UGOVORA

5.1 CASE STUDIES OF SMART CONTRACT USAGE

Once the fundamental characteristics and technical architecture of smart contracts have been defined, it is important to present their practical application in various areas of digital services. The following examples and case studies demonstrate how the theoretical principles and functional capabilities of smart contracts are implemented in practice through specific platforms and systems.

DeFi: A well-known example of smart contract implementation in decentralised finance is the MakerDAO platform [17], which enables the issuance of the stable cryptocurrency DAI based on collateralized deposits. Smart contracts automatically manage liquidation and collateral, ensuring system stability without the need for a centralised intermediary. Similarly, platforms such as Compound use contracts to automatically determine interest rates and distribute liquidity among users.

Supply chains: In the IBM Food Trust system [22], blockchain and smart contracts are used to track the provenance of food and verify product authenticity. Contracts automatically record deliveries and certifications, increasing transparency and trust between suppliers and consumers.



Slika 2 *Primjer decentraliziranog postupka kreditiranja upotrebom pametnoh ugovora.*

Figure 2 *An example of a decentralized lending process using smart contracts.*

Healthcare: The MedRec project [23], developed at MIT, uses smart contracts to manage access to medical records. Through the blockchain, patients control who can access their data, enabling decentralised privacy management and interoperability between healthcare institutions.

Public administration: Pilot projects such as Estonia's e-Residency programme [24] use smart contracts for identity verification. These projects demonstrate the technology's potential to reduce bureaucracy and increase the transparency of public processes.

These examples show that the application of smart contracts goes beyond conceptual frameworks and is becoming a practical tool for shaping new models of business and public services. The analysis of real-world implementations confirms that the success of digital solutions largely depends on the technical design of contracts, the choice of platform, and the application context, further emphasising the need to integrate technological and methodological approaches in future research.

6. IZAZOVI, OGRANIČENJA I EVOLUCIJA PAMETNIH UGOVORA

6. CHALLENGES, LIMITATIONS, AND EVOLUTION OF SMART CONTRACTS

Smart contracts face significant barriers to adoption. Technical limitations such as poor scalability, immutability risks, and reliance on oracles constrain performance. Security vulnerabilities make rigorous audits essential but costly. Legal uncertainty also persists: enforceability varies by jurisdiction, and automated execution often conflicts with traditional dispute resolution. Interoperability remains limited due to fragmented platforms and the lack of universal standards. Socioeconomic barriers, including complex user interfaces, reliance on developers and oracles, and unequal access to infrastructure, risk exacerbating digital inequalities.

Future development of smart contracts focuses on greater automation, interoperability, and governance. Integration with artificial intelligence and the Internet of Things (IoT) could enable autonomous services in areas such as predictive maintenance and smart cities, although explainability and compliance remain challenges [16]. Interoperability among different blockchain platforms will allow contracts to function across multiple platforms, supporting complex services across domains. Progress in regulation and "compliance by design" will strengthen legal enforceability and support adoption in finance and healthcare. Efforts by ISO and EEA in standardisation aim to improve interoperability, security, and cost-effectiveness through verification tools and reusable templates. Governance models are evolving through decentralised autonomous organisations (DAOs), with hybrid approaches and mechanisms such as quadratic voting promising more inclusive and resilient decision-making [16, 17].

7. ZAKLJUČAK

7. CONCLUSION

Smart contracts have become the foundation of digital service innovation, providing automation, transparency, and trust minimisation that far surpass traditional centralised models. Their use in finance, supply chains, healthcare, digital identity, and public services demonstrates their versatility and transformative potential. However, ongoing challenges such as scalability, security risks, legal recognition, interoperability, and socioeconomic barriers underscore the need for continued technical refinement, regulatory development, and inclusive design.

Looking ahead, advances in cross-chain interoperability, integration with artificial intelligence and the Internet of Things, and the creation of standardised frameworks and governance models are set to expand the scope and reliability of smart contracts. By addressing these challenges while building on their unique strengths, smart contracts are likely to play a decisive role in shaping the next generation of secure, efficient, and responsible digital services.

8. REFERENCE

8. REFERENCES

[1.] Crosby M.; Pattanayak P.; Verma S.; Kalyanaraman V.; "Blockchain Technology: Beyond Bitcoin," Applied Innovation Review, vol. 2, pp. 6–19, 2016. ISSN: 2504-0385.

[2.] Nakamoto S.; "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[3.] Buterin V.; "A Next-Generation Smart Contract and Decentralized Application Platform," Ethereum White Paper, 2014. [Online]. Available: https://ethereum.org/en/whitepaper/

[4.] Christidis K.; Devetsikiotis M.; "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2016, doi: 10.1109/ACCESS.2016.2566339. ISSN: 2169-3536.

[5.] Casino F.; Dasaklis T. K.; Patsakis C.; "A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues," Telematics and Informatics, vol. 36, pp. 55–81, Mar. 2019, doi: 10.1016/j.tele.2018.11.006. ISSN: 0736-5853.

[6.] Tapscott J.; Tapscott D.; Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. New York, NY, USA: Penguin, 2016. ISBN: 978-1101980132.

[7.] Swan M.; Blockchain: Blueprint for a New Economy. Sebastopol, CA, USA: O'Reilly Media, 2015. ISBN: 978-1491920497.

[8.] Wang W.; Hoang D. T.; Hu P.; Xiong Z.; Niyato D.; Wang P.; Wen Y.; "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks," IEEE Access, vol. 7, pp. 22328–22370, 2019, doi: 10.1109/ACCESS.2019.2896108. ISSN: 2169-3536.

[9.] Buterin V.; "Ethereum White Paper," 2014. [Online]. Available: https://ethereum.org/en/whitepaper/

[10.] Schär F.; "Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets," Federal Reserve Bank of St. Louis Review, vol. 103, no. 2, pp. 153–174, 2021, doi: 10.20955/r.103.153-74. ISSN: 0014-9187.

[11.] Szabo N.; "The Idea of Smart Contracts," 1997. [Online]. Available: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_idea.html

[12.] Atzei N.; Bartoletti M.; Cimoli T.; "A Survey of Attacks on Ethereum Smart Contracts," in Principles of Security and Trust (POST 2017), LNCS 10204, Springer, 2017, pp. 164–186, doi: 10.1007/978-3-662-54455-6_8. ISBN: 978-3-662-54454-9.

[13.] Melo, C., Gonçalves, G., Silva, F.A. et al. "A comprehensive hyperledger fabric performance evaluation based on resources capacity planning," Cluster Comput 27, 12395–12410 (2024). https://doi.org/10.1007/s10586-024-04591-4

[14.] Tudor Ferariu, Philip Wadler, and Orestis Melkonian. "Validity, Liquidity, and Fidelity: Formal Verification for Smart Contracts in Cardano," In 6th International Workshop on Formal Methods for Blockchains (FMBC 2025). Open Access Series in Informatics (OASIcs), Volume 129, pp. 6:1-6:21, Schloss Dagstuhl – Leibniz-Zentrum für Informatik (2025) https://doi.org/10.4230/OASIcs.FMBC.2025.6

[15.] Ashraf, M., & Heavey, C. (2023). "A prototype of supply chain traceability using Solana as blockchain and IoT integration," Procedia Computer Science, 217, pg. 948-959.

[16.] Abbas, H., Caprolu, M., & Di Pietro, R. (2022). "Analysis of Polkadot: Architecture, Internals, and Contradictions," arXiv preprint arXiv:2207.14128.

[17.] MakerDAO; "The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System," White Paper, 2020. [Online]. Available: https://makerdao.com/en/whitepaper/

[18.] Kshetri N.; "Blockchain's Roles in Meeting Key Supply Chain Management Objectives," International Journal of

Information Management, vol. 39, pp. 80–89, Apr. 2018, doi: 10.1016/j.ijinfomgt.2017.12.005. ISSN: 0268-4012.

[19.] Azaria A.; Ekblaw A.; Vieira T.; Lippman A.; "MedRec: Using Blockchain for Medical Data Access and Permission Management," in Proc. 2nd Int. Conf. Open Big Data (OBD), Vienna, Austria, 2016, pp. 25–30, doi: 10.1109/OBD.2016.11. ISBN: 978-1-5090-2948-9.

[20.] Zyskind G.; Nathan O.; Pentland A.; "Decentralizing Privacy: Using Blockchain to Protect Personal Data," in 2015 IEEE Security and Privacy Workshops, San Jose, CA, USA, 2015, pp. 180–184, doi: 10.1109/SPW.2015.27. ISBN: 978-1-4673-6949-7.

[21.] Ølnes S.; Ubacht J.; Janssen M.; "Blockchain in Government: Benefits and Implications of Distributed Ledger Technology for Information Sharing," Government Information Quarterly, vol. 34, no. 3, pp. 355–364, Sept. 2017, doi: 10.1016/j.giq.2017.09.007. ISSN: 0740-624X.

[22.] IBM. (2019). "IBM Food Trust: How Blockchain Digitally Transforms Food Chains, " [White paper]. IBM Corporation. Retrieved from https://www.amcham.gr/wp-content/uploads/2019/11/LINARDAKHS_4thEUF.pdf

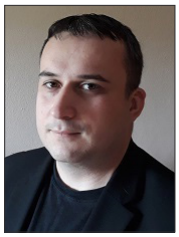
[23.] Ekblaw, A. "MedRec: Blockchain for Medical Data Access, Permission Management and Trend Analysis," MIT Media Lab. Retrieved [10/2025], from https://www.media.mit.edu/publications/medrec-blockchain-for-medical-data-access-permission-management-and-trend-analysis/

[24.] Sullivan, C. & Burger, E. "E-residency and blockchain,", Computer Law & Security Review, vol. 33, no. 4, 2017, DOI: https://doi.org/10.1016/j.clsr.2017.03.016

AUTORI · *AUTHORS*

• **Aleksandar Stojanović** - Nepromijenjena biografija nalazi u časopisu P&D, Svezak. 11, Br. 4 iz 2023. godine.

Korespondencija · *Correspondence*
aleksandar.stojanovic@tvz.hr



• **Željko Kovačević** - Biografija autora nalazi se na web stranicama https://nastava.tvz.hr/zkovacevic/.

Korespondencija · *Correspondence*
zeljko.kovacevic@tvz.hr

• **Maja Dabčević** - Studentica je pete godine Informacijske sigurnosti i digitalne forenzike na Tehničkom veleučilištu u Zagrebu. Trenutno je zaposlena na radnom mjestu razvojnog inženjera u poduzeću Innovez d.o.o. U slobodno vrijeme razvija vlastite projekte te sudjeluje na raznim aktivnostima i natjecanjima u sklopu Veleučilišta.