

Smart contract in security

Nikolay Radulov, Teodora Lichev
New Bulgarian University
n.stefanov5@gmail.com, teodora_licheffa@abv.bg

Abstract: This comprehensive document explores the role and implementation of smart contracts in security systems, with particular emphasis on their application in law enforcement, intelligence, and counterintelligence operations. The analysis covers both theoretical foundations and practical applications within Industry 5.0 context.

Keywords: Blockchain; Smart contract, Intelligence; Security

1. Introduction

Smart contracts are self-contained computer programs that automatically execute, manage, or verify the terms of contractual agreements using blockchain technologies. Their significance in the context of Industry 5.0 and security is particularly important as they contribute to new norms of data protection and transparency in business operations.

Blockchain technology is the fundamental foundation for the functioning of smart contracts and offers numerous advantages and unique features that make these two concepts interconnected and complementary. In the following lines, we will examine the features, properties and specificities of blockchain technology that make it an ideal platform for the execution of smart contracts.

2. Features of blockchain technology

The blockchain functions as a single and reliable source of information with the following characteristics:

Decentralization:

Blockchain is a decentralized platform, which means that there is no single controlling authority. Instead, data and information are distributed across multiple nodes that interact with each other. Adding a piece of information requires all nodes on the blockchain to agree and approve it. This reduces the risk of manipulation and abuse due to the lack of central control.

Immutability

Once information is on the blockchain, it cannot be changed or deleted without leaving a trace, and without these changes being approved by all participants in the chain. Each block contains information about the previous block, making the system extremely resistant to attempts at manipulation.

Transparency

All transactions and operations performed on the blockchain are publicly available and visible to network participants. This provides a high degree of transparency, allowing anyone to track the history of transactions and smart contracts.

Cryptographic security

Blockchain uses cryptographic security methods, which increases the protection of data and transactions. Each block is provided with a unique hash, and the data in it is encrypted, which prevents unauthorized access and manipulation. A hash contains 64 characters and is a combination of 26 letters and 10 numbers.

3. Properties of Blockchain

Auto-executed:

Smart contracts implemented on a blockchain platform work automatically if the specified conditions are met.

Intelligent contracts (also called smart contracts – from the English. Smart Contracts) are electronic contracts that are written in blockchain code and are based on the "if / when ... then ..." function

This means that under certain conditions, the contract automatically performs pre-set actions, without the need for human intervention.

Proof of performance:

Every transaction and execution of smart contracts is recorded on the blockchain, providing conclusive proof of actions. This feature is of great importance for resolving disputes or verifying the legality of actions.

Low cost and speed:

Process automation through smart contracts, combined with blockchain technology, can reduce execution costs and transaction processing times. Without the need for intermediaries, the costs of services related to bureaucracy and paperwork are significantly reduced.

4. Specifics of blockchain and smart contracts

Cross-vertical integration

Blockchain enables the integration of different sectors and industries, which provides flexibility in the application of smart contracts. They can be applied in a variety of areas — from financial services to supply management and healthcare.

Proof of authenticity

Blockchain ensures the integrity and authenticity of information. Every contract or transaction made on a blockchain is given a unique identifier that confirms its legitimacy. Once added to the blockchain, it is almost impossible for the information to be manipulated, deleted, or

Identity Management

Blockchain can be used for digital identity management, allowing participants in smart contracts to verify their identities without the need for centralized authorities. This provides advantages in terms of security and protection of personal and sensitive data.

Blockchain technology provides a solid foundation for the functionality of smart contracts, offering decentralization, immutability, transparency, and security. These properties and features make blockchain extremely suitable for integrating smart contracts into various industries and applications, with the potential to transform the way transactions and interactions between participants are carried out. The importance of blockchain for smart contracts cannot be underestimated, as it not only provides the necessary infrastructure, but also offers mechanisms for safe and trusted interaction.

5. Essence and content of smart contracts

Smart contracts, as mentioned above, operate on the blockchain, which allows them to be tamper-proof and offer a high level of security. They require predefined conditions, programmable in languages such as Solidity for Ethereum, which are automatically executed when certain criteria are met. The content of smart contracts usually includes logic that describes the terms of the transaction, what actions to take in different situations, and how the system should respond to changes.

Form

Smart contracts do not have a physical form, they are a complex of programmed codes located on the blockchain. This form provides not only security, but also decentralization, since the information cannot be changed from a central location. Any participant in the network can check the terms and status of the contract, ensuring transparency.

Opportunities

Smart contracts offer numerous security opportunities, including but not limited to:

- Automation: Processes become automated, which reduces the need for third-party intervention.
- Cost reduction: Removing intermediaries leads to lower operational costs.
- Increased security: The use of cryptography in blockchain technologies provides high data protection.

- Speed: Processes are performed in near real-time, which increases the efficiency of business practices.

Challenges and problems

Despite their many advantages, smart contracts also face several challenges:

- Legal and regulatory issues: The lack of a clear legal framework regarding smart contracts may be an obstacle to their widespread adoption.
- Technical barriers: Implementing complex smart contracts requires specialized IT skills, which can be a barrier for small businesses.
- Fault tolerance: If the terms of the contract are not properly programmed, they can lead to unintended consequences.

Efficiency

The effectiveness of smart contracts in Industry 5.0 is manifested by improving process transparency, accelerating transactions, and reducing costs. By optimizing operational activities, smart contracts enable the organization of activities based on real, verifiable data, thereby achieving sustainable business performance that meets the requirements of Industry 5.0 for sustainability and human orientation.

Smart contracts in the context of Security 5.0 present an innovative tool for managing business relationships and protecting data, significantly improving market dynamics, but also posing several challenges that require attention and resolution.

The use of smart contracts in the management of security services, such as the police, intelligence and counterintelligence, is an innovation that could lead to significant improvements in operational efficiency, transparency and security of information processes. In the following lines, we will examine how smart contracts can be integrated into these systems and what positive and negative effects they can have.

6. Smart contracts in the police

Automated data management: Police handle large amounts of information, such as reports and evidence. Smart contracts can be used to automate the storage, sharing, and verification of documents and data. Blockchain ensures the correct and secure digitization of inheritance records and registries. For example, when a new legal norm is implemented, smart contracts could automatically update databases and notify the relevant authorities.

Informant Contract Management: Police often work with informants who provide valuable information. Smart contracts can be used to formalize relationships with informants, providing automated payments for reporting important information. These contracts could include provisions to protect the anonymity and safety of the informant.

Regulating cooperation with other agencies: Smart contracts can define the terms of cooperation between different security services and international agencies. The parameters of cooperation, information exchange, and resource allocation can be strictly fixed and monitored through smart contracts.

7. Smart contracts in intelligence

Secure communication channels: Intelligence agencies work with sensitive information. Smart contracts can provide structured and encrypted channels for information exchange between agents, which would increase data security and reduce the risk of espionage, information leaks, or malicious actions.

Risk monitoring and assessment: Intelligence often involves threat and vulnerability assessment. Smart contracts can automate the process of collecting and analyzing risk data, providing intelligence officers with up-to-date and accurate threat data.

Systems Integration: Smart contracts can be implemented into various platforms and systems used by intelligence agencies to improve interaction and coordination between different divisions and services.

8. Smart contracts in counterintelligence

Automated identity verification: Counterintelligence needs to monitor and verify multiple identities. Smart contracts can be used to automate background checks, which would help prevent potential espionage threats.

Covert Operations Management: Smart contracts can automate projects and funding of covert operations, reducing the risk of exposure and abuse by providing detailed tracking of every phase of the operation.

Accountability and transparency: By implementing smart contracts in counterintelligence operations, accountability and the possibility of subsequent checks are ensured, useful for preventing abuse and illegal actions.

Challenges and problems

Despite the many advantages, the introduction of smart contracts in security services is accompanied by several challenges:

- **Legal and ethical issues:** The implementation of automated data management and action systems may encounter resistance related to legal regulations and data protection. Clear frameworks and guidelines are needed for the use of smart contracts in sensitive areas. The ultra-rapid development of technologies significantly exceeds legislative initiatives and frameworks to regulate their use.

- **Technical hurdles:** Integrating new technologies into legacy security systems can be challenging, especially when it comes to training employees and adapting existing infrastructure. Most information systems are built in a way that they are not compatible, and data migration is a challenge.

- **Cybersecurity:** Although blockchain provides a high level of protection, systems still remain vulnerable to attacks. The strength of smart contracts depends on the strength of the blockchain infrastructure and the network itself.

Smart contracts offer significant opportunities to enhance the efficiency and security of security services, but their implementation requires a careful balance between innovation, legal regulations and ethical considerations. The success of such initiatives will depend on active partnerships between technological companies, government institutions and public organizations aimed at building transparent and fair systems that support public safety and protection.

Management

Smart contracts offer a new, innovative approach to security management. By integrating blockchain technology and automating contractual relationships, these tools can significantly improve management efficiency in various areas, including policing, intelligence, and counterintelligence.

In the following lines, we will examine how smart contracts can be incorporated into every phase of the governance cycle, with particular emphasis on their specific application in the security sector.

Analysis

Analysis is a fundamental step in the management cycle, where current conditions, resources, and problems are assessed. Smart contracts can help in this phase by automatically collecting and processing data from various sources.

- **Data collection:** Smart contracts can automatically extract and analyze information from numerous databases, including information about previous cases, criminal records, and data from intelligence operations.

- **Vulnerability Assessment:** By analyzing live data, they can identify security vulnerabilities by automatically generating risk reports.

Forecasting

After analysis, the next step is to predict future trends and threats. Smart contracts can provide important information based on reliable data and algorithms.

- **Threat Modeling:** By applying algorithms and machine and deep learning, smart contracts can predict future threats and criminal activities based on historical data.

- Scenario planning: Automatic data processing can help in developing different threat scenarios, which will inform security management.

Decision making

Based on the analysis and predictions, the decision-making stage follows. Smart contracts can provide real-time information to facilitate the decision-making process.

- Objectivity in decisions: Smart contracts guarantee transparency and objectivity in decision-making, as all conditions and criteria are predetermined and clearly formulated.

- Automated solutions: Under certain conditions set in their programming, smart contracts can trigger certain actions themselves, for example, notifying the relevant authorities of attempted security breaches.

Planning

Planning is a critical stage for which smart contracts can provide significant added value.

- Strategic Planning: Smart contracts can be used to automate planning processes related to resource deployment, operations management, and conduct training modules.

- Budget Management: Through automated expense reports and commitments, smart contracts can improve financial planning by pragmatically determining the costs of various operations based on previous executions.

Organizing

Organizing resources and operations is key to the successful functioning of security services. Smart contracts can increase the efficiency of resource management.

- Resource Optimization: Smart contracts can automatically determine how and where to use available resources to achieve maximum efficiency.

- Coordination between teams: Smart contracts can automate communication and coordination between different departments and teams, providing a platform for information exchange while minimizing the risk of errors.

Control

Control is the final stage of the management cycle and is of utmost importance, especially in security management.

- Performance Monitoring: Smart contracts can track the execution of certain tasks and conditions, automatically providing reports on performance and regulatory compliance.

- Preventing violations: The control system, powered by smart contracts, can automate alerts when anomalies or unmet conditions are identified, allowing for rapid response from management.

The integration of smart contracts into security management offers unique opportunities to increase efficiency, transparency, and security. By automating key management functions, such tools can not only improve operational performance but also instill more trust in decision-making processes. Despite the prospects, it is important to put in place adequate legal and ethical frameworks to ensure that the implementation of smart contracts does not violate personal rights and good practices in the field of security.

Smart contracts a tool for humanity and ethics

Smart contracts can play a significant role in the implementation of special intelligence tools (SIPs), especially when it comes to ensuring legality and compliance with ethical standards. Through automation and transparency, they can help protect both citizens and security service personnel. In the following, we will examine how smart contracts can provide the necessary legal prerequisites for the use of special intelligence tools.

Determining the legal conditions

The smart contract can be programmed to contain specific details regarding the legal conditions required to activate the special intelligence tools. These conditions should include:

- Clear criteria: Defining specific cases in which SRCs can be used, such as the presence of evidence of serious crimes or threats to national security.

- Legal permissions: A smart contract may require prior approval from competent authorities (such as a court) before activating the SCC, ensuring legality.

Automate approvals

Smart contracts can automate the approval process by integrating mechanisms to verify legal conditions:

- Integration with legal databases: Smart contracts can connect to central legal databases to verify the availability of necessary permits and approvals in each individual case.

- Launch conditions: The smart contract can be structured to only start after validating the legal conditions, automatically recording the data integration.

Control and monitoring of implementation

Smart contracts offer mechanisms for control and monitoring during the implementation of special intelligence tools:

- Activity Tracking: Whenever CPCs are activated, the contract can record the time, method of activation, and subsequent usage, thus providing the necessary transparency and accountability.

- Notifications: The smart contract can automatically send notifications to responsible authorities and control institutions upon activation of the SRC, thus ensuring access to information and monitoring.

Conditions for termination of operations

The smart contract may also include mechanisms to automatically terminate SRC operations if certain conditions are not met or violated:

- Data analysis: The smart contract can analyze data in real time and terminate the operation if, for example, no suspicious activities are detected within a certain period.

- Reporting requirements: After termination of the operation, the smart contract can generate a report of the activities performed to be shared with the authorities responsible.

Protection of citizens and employees

Through the listed mechanisms, smart contracts serve as a protective barrier for both citizens and security service employees:

- Transparency and accountability: Ensuring monitoring and accountability prepares scenarios that show clear responsibility of employees for the implementation of the SRC, which reduces the risk of abuse. Smart contracts can perform routine processes in the work cycle and employees can concentrate on specialized and expert work.

- Legal protection for employees: Smart contracts provide protection for employees from unintentional violations of the law. In the event of an improper application of the SRC, the contract can provide evidence of the actions taken, including the time and conditions of activation.

Smart contracts offer an innovative solution for the legal and ethical application of special intelligence tools in the security sector. By automating legal conditions, dynamic risk assessment, and transparency of actions, they can ensure the protection of the rights of both citizens and employees. This automation creates a new norm of accountability and legal compliance necessary for the modernization of intelligence structures, strengthening public trust and the effectiveness of security services.

Smart contracts represent a key innovation that has the potential to support the realization of concepts such as humanity, ethics and human-centeredness in the context of Security 5.0. This new era of security emphasizes not only technology and automation, but also social responsibility and protection of individual rights. As a basis for smart contracts, we can consider the following aspects:

Humanity and protection of rights

Smart contracts offer mechanisms that protect citizens' rights and ensure that technological innovations in security are aimed at

ensuring the well-being of society. They can be programmed with extreme attention to ethical standards:

- Automation of Justice: Through smart contracts that automatically check legal requirements, violations of individual rights can be prevented. For example, the use of special intelligence tools (SIPs) can be automated and controlled in a way that ensures compliance with legal and ethical norms.
- Access to justice: Smart contracts can streamline processes and reduce the cost of legal services, which would allow more citizens to gain access to justice and legal protection.

Ethics in processes

Smart contracts can be programmed to follow specific ethical principles, which provide greater transparency and accountability in the management of data and resources:

- Transparency and accountability: Smart contracts offer an immutable record of action, always allowing for verification of the authenticity of the procedure. This is especially important in the security field, where unethical practices can lead to significant social and legal consequences.
- Consent and awareness: Through smart contracts, participants in the system can give consent to the processing of personal data, and contracts themselves can encrypt and protect data, ignoring consent whenever informational conditions are not met.

Human-centeredness and focus on the individual

At the heart of Security 5.0 is the concept of human-centricity, which puts individuals and their needs first. Smart contracts can play a critical role in this dynamic:

- Personalized Services: Smart contracts offer the opportunity to tailor individual services provided to citizens. For example, in public safety management, personalized smart contracts can reflect the needs of the respective community, ensuring more effective and targeted measures.
- Community engagement: Smart contracts can provide a platform for citizen participation in decision-making processes, giving them a voice and participation in the management of local security initiatives.

Sustainability and integrity

The resilience and integrity of systems in Security 5.0 can be strengthened through smart contracts that provide durable and sustainable solutions to security problems:

- Supporting sustainable development: Smart contracts can be programmed to implement sustainable development principles, such as managing security resources in a way that minimizes negative impact on the environment and society.
- Data integrity: By protecting data from manipulation and unjustified changes, smart contracts ensure the integrity of the information needed for security services to make informed decisions.

Conclusion

Smart contracts play an important role in promoting humanity, ethics, and human-centeredness in the Security 5.0 ecosystem. They offer mechanisms to protect citizens' rights, ensuring transparency and accountability, as well as the possibility of personalized and sustainable security management. The importance of these aspects is essential for building trust between citizens and government institutions and for creating safe and fair public systems. With the help of smart contracts, we can achieve a balance between technological innovation and ethical obligations to individuals and the community.

Literature

1. Личева, Т. „Сигурност на данните с блокчейн технологията” В. Сб. Док. от годишната научна конференция на ВТУ „Васил Левски” – 8-9 юни 2023 г., ISSN 2367-7481, с. 383
2. Личева, Т. Модерна сигурност в управлението, изд. 2023, НТС по машиностроене „Индустрия 4.0”, ISBN 978-619-7383-30-0, с. 61
3. Радулов, Н., „Сигурност 4.0“, 2019, изд. Научнотехнически съюз по машиностроене „Индустрия 4.0, ISBN 978-619-7383-15-7 стр.307-309
4. A Guide to Smart Contract Security, <https://hedera.com/learning/smart-contracts/smart-contract-security>
5. Blockchain-based smart contracts as new governance tools for the sharing economy, <https://www.sciencedirect.com/science/article/abs/pii/S0264275121002250>
6. How smart contracts will change the way the world works, <https://www.deltacapita.com/insights/how-smart-contracts-will-change-the-way-the-world-works>
7. Smart Contracts for Estate Planning and Administration, <https://susqblockchain.medium.com/smart-contracts-for-estate-planning-and-administratio-c400114e8a58>
8. The Future of Smart Contracts: Trends and Predictions, <https://www.rapidinnovation.io/post/the-future-of-smart-contracts-trends-and-predictions>
9. Blockchain Technology in Law Enforcement and Security: Overview, <https://www.ijraset.com/research-paper/blockchain-technology-in-law-enforcement-and-security>
10. How smart contracts work with blockchain, <https://www.britannica.com/money/how-smart-contracts-work>
11. Human-Centric Collaboration and Industry 5.0 Framework in Smart Cities and Communities: Fostering Sustainable Development Goals 3, 4, 9, and 11 in Society 5.0, <https://www.mdpi.com/2624-6511/7/4/68>