**Lit. Review**

**Intelligent Smart Contracts for Innovative Supply Chain Management**

**Abstract**

The paper proposes using blockchain-based intelligent smart contracts to enhance trust, coordination, and automation in supply chain management. These smart contracts would enable autonomous decision-making to improve collaboration and profitability among supply chain partners. The authors outline a new blockchain-driven supply chain architecture based on algorithmic methodologies that would allow intelligent contracts to automatically execute tasks and optimize operations.

**Method**

The paper proposes a novel supply chain management approach using blockchain technology and intelligent smart contracts that automate execution and coordination. The authors detail the algorithmic methodologies that would allow these smart contracts to make autonomous optimizations and decisions. A core component is the implementation of a Revenue Sharing (RS) methodology enabled by the blockchain platform, which distributes proceeds fairly among supply chain partners to incentivize efficiency and collaboration. By establishing algorithmic trust, the blockchain architecture reduces the need for central control and power asymmetries. The paper outlines how this reimagined supply chain system founded on intelligent contracts, revenue sharing, and decentralized trust could lead to increased profitability, cooperation, and widespread economic benefits for participating enterprises. Overall, the combination of technical innovation and collaborative incentives aims to address fundamental coordination and trust issues in supply chain networks.

**Result**

The paper puts forth an innovative blockchain-based approach to enhance supply chain management through automated smart contracts and decentralized trust. The authors propose "intelligent smart contracts" running on blockchain that can autonomously execute tasks, adjust costs, and replace human managers, thereby streamlining operations. To incentivize efficiency and fairness, a Revenue Sharing (RS) methodology is suggested to distribute proceeds among all supply chain partners. This collaborative model is enabled by a blockchain platform that establishes algorithmic trust, eliminating the need for central control. By leveraging blockchain's decentralized architecture, power asymmetries and intermediaries can be removed from supply chain networks. The proposed system aims to increase profitability, cooperation, and economic prosperity for participating enterprises by addressing fundamental coordination and trust issues. Overall, the combination of intelligent contracts, revenue sharing, and blockchain promises major benefits through automated, optimized supply chain workflows founded on decentralized consensus.

**Conclusion**

The paper proposes the use of blockchains and smart contracts as enabling technologies for an innovative type of supply chain management, aimed at achieving higher levels of collaboration between the companies participating in the chain. The authors introduce the concept of Intelligent Smart Contract, which is a contract executable on the blockchain and characterized not only by "smartness" but also by "intelligence." They illustrate a specific instance of an intelligent smart contract, both from an algorithmic and an architectural standpoint, as given by Revenue Sharing, a methodology for supply chain management that can greatly boost the profitability of the supply chain for the benefit of all participants. The paper concludes that the proposed intelligent smart contracts can replace human trusted third parties in coordinating the various parties in the management of a supply chain, making it much easier and less expensive to set up supply chains based on peer-level participation.

**Future work**

The paper outlines two key areas for future work - technological and organizational. On the technology side, further research is needed to quantify the transaction cost improvements from adopting blockchain-enabled digital trust. Additional work could optimize intelligent smart contracts like the proposed Revenue Sharing model and dynamically create supply agreements between new partners. Organizationally, more study is required on how this approach would impact different supply chain players. Currently, larger enterprises benefit most from outsourcing and utilizing information technology and legal tools. The authors suggest Intelligent Smart Contracts and Revenue Sharing could move towards a more cooperative process that distributes benefits across the supply chain, not just favoring major players. This has the potential to level the playing field for smaller parties. Overall, future technological and organizational research should continue exploring blockchain's impacts on transaction costs, automated agreements, and equitable profit sharing to refine this reimagined supply chain architecture.

**Artificial Intelligence, Smart Contracts and Islamic Finance**

**Abstract**

The paper explores the potential impact of artificial intelligence (AI) and smart contracts on Islamic finance. It explains how AI can simulate human decision-making while smart contracts automatically execute transactions through coded programming. By comparing the functionality of these technologies, the study concludes they will significantly shape the future of Islamic finance by driving efficiency, reducing human involvement, and enabling automation. Specifically, smart contracts offer advantages over traditional agreements by self-executing based on predefined rules. Their application across healthcare, real estate, securities, and other sectors can streamline financial systems by minimizing friction and intermediaries. Overall, the paper argues AI and smart contracts will bring major innovations to Islamic finance through their capabilities to replicate human intelligence and automatically govern interactions between parties.

**Method**

N/A

**Result**

The paper concludes that artificial intelligence (AI) and smart contracts will substantially impact the future of Islamic finance. AI can simulate human decision-making and even surpass it in areas like radiology, reducing mistakes in banking services through automation. Meanwhile, smart contracts offer efficiency, selective visibility, and data enrichment, with applications across banking, insurance, energy, e-government, and more. Together, AI and smart contracts can enhance accuracy, minimize errors, and optimize data management for organizations. AI's automation can replace human judgement and involvement in processes like auditing and fraud detection. And smart contracts' blockchain integration enables credible, transparent transactions. With improved accuracy, efficiency and experiences, the combination of these technologies will shape the future of Islamic finance. Customers can expect more streamlined, transparent and satisfying banking powered by the automation and capabilities of AI and smart contracts. This represents a major modernization of services.

**Conclusion**

The paper concludes that artificial intelligence (AI) and smart contracts will profoundly transform the Islamic finance industry going forward. It notes AI's capacity to simulate human decision-making while smart contracts can enable credible and authenticated transactions without paper contracts. This digital approach is poised to revolutionize banking and commerce. Together, AI and smart contracts can boost accuracy, reduce errors, and enhance data management across organizations. By leveraging these technologies, banks can better meet rising customer expectations through improved experiences. The automated intelligence of smart contracts and AI's ability to replace human functions can minimize friction and overhead in financial transactions. Overall, the paper argues Islamic finance will see significant enhancements from integrating AI and blockchain-based smart contracts that increase credibility, efficiency, and customer satisfaction. This represents a major modernization of traditional systems.

**Future work**

The paper proposes several fruitful research directions to build on the transformative potential of AI and smart contracts for Islamic finance. Specific applications could be explored in risk analysis, fraud detection, and compliance where automation can assist human tasks. Chatbots leveraging natural language AI may enhance customer service through efficient, personalized interactions. Integrating smart contracts and AI with other emerging technologies like big data, cloud computing, and robotics could further bolster capabilities and efficiency gains. Legal and regulatory implications require study too, including contract enforceability, dispute resolution, and privacy with smart contracts. Additionally, research should examine the challenges and risks of adopting these technologies such as ethical issues, cybersecurity, and workforce impacts. Overall, future research can further delineate the applications of AI and smart contracts in Islamic finance, while also investigating critical questions around regulation, ethics, security, and social welfare.

**A novel extended multimodal AI framework towards vulnerability detection in smart contracts**

**Abstract**

The paper puts forth a novel methodology for testing smart contracts using whitebox knowledge and supervised multimodal learning. It extracts code and graph embeddings at the single modality level, then combines these into a joint multimodal feature representation. This allows detecting vulnerabilities by analyzing smart contracts through multiple integrated modes. The approach is evaluated on a dataset of over 100,000 functions, achieving up to 99.71% detection performance. By enabling deep integrated analysis of code, structure, and execution paths, the multimodal framework significantly outperforms single modality methods. The proposed technique advances smart contract security by leveraging diverse complementary views of contract characteristics and behavior. Through supervised learning and fusion of code, graph, and runtime embeddings, the methodology provides a robust way to identify vulnerabilities and flaws in smart contracts prior to deployment.

**Method**

The paper proposes a smart contract testing methodology incorporating whitebox knowledge and supervised multimodal learning for detecting vulnerabilities. It utilizes static analysis and a series of tasks including feature selection, dimension unification, feature fusion, model training, and decision-making. The approach leverages multiple features such as code and graph embeddings at both intramodal and intermodal levels. State-of-the-art machine learning models like self-attentive bi-LSTM, textCNN, and random forest are trained to extract a unified multimodal representation for each task. The framework is evaluated on a dataset of over 100,000 functions from SmartEmbed, ranking the performance of different multimodal strategies. The highest detection performance achieved is 99.71%, demonstrating the effectiveness of fusing diverse views of code, structure, and execution paths for robust vulnerability identification in smart contracts.

**Result**

The proposed framework is evaluated on over 100,000 functions from the SmartEmbed dataset. It achieves exceptional vulnerability detection, with the highest performance reaching 99.71% across different strategies. The paper ranks each multimodal mining approach, finding the framework outperforms existing schemes. Comparisons at the SC, BB, and EVMB layers showcase top strategies and models. At the SC layer, strategy 7 leveraging bi-LSTM self-attention and Random Forest is optimal. For the BB layer, combining SSA-W2V, SSA-Bert, and BB-CFG features with strategy 7 surpasses the AME-VulDetector. Finally, strategy 9 using bi-LSTM self-attention and Dense stack on EVMB-CFG2 outperforms DGCNN and other methods at the EVMB layer. The comprehensive performance benchmarks demonstrate the framework's effectiveness in fusing static analysis, machine learning, and multi-layer contract embeddings to reliably detect vulnerabilities with up to 99.71% accuracy across various smart contract components.

**Conclusion**

The paper presents a novel smart contract vulnerability detection framework using a multimodal AI approach with whitebox knowledge and supervised learning. It extracts code and graph embeddings at single and intermodal levels, feeding them into advanced models like bi-LSTM, textCNN, and random forest for feature extraction and detection. Tested on over 100,000 functions, the framework achieves exceptional 99.71% detection performance, outperforming existing schemes. The paper concludes that combining multimodal features from different smart contract layers provides customizable and flexible strategies that boost detection. It also shows three-by-three intermodal fusion outperforms two-by-two and intramodal settings. Future work is suggested to address out-of-vocabulary issues, enable multi-class classification, and explore feature importance. Overall, the proposed framework advances the state-of-the-art in smart contract security through its innovative integration of static analysis, graph representations, deep learning, and multimodal feature fusion to reliably identify vulnerabilities.

**Future work**

The paper outlines several areas for future research to build on the proposed multimodal vulnerability detection framework. One direction is addressing the out-of-vocabulary issue that arises when unseen identifiers are encountered during static analysis. Enabling multi-class classification of different vulnerability types is also proposed to expand beyond binary detection. Additionally, diving deeper into feature importance could elucidate which code, graph, and execution embeddings most influence successful vulnerability identification. This can guide feature engineering and selection to further optimize the detection model. Overall, the suggested future work aims to refine the framework by handling unseen data, classifying vulnerability categories, and determining the most salient features for detection. Advancing these areas will strengthen the framework and provide greater insight into multimodal deep learning for robust smart contract security.

**AI-powered Smart Contracts: The Dawn of Web 4.0**

**Abstract**

The paper discusses how integrating artificial intelligence with smart contracts can overcome limitations of static contracts and enable new capabilities. Smart contracts with built-in AI can adapt to changing conditions, monitor for attacks, and decentralize marketing using incentives. AI enables applications like gaming fashion design on the blockchain. Additionally, combining AI and blockchain can revolutionize real estate by securing asset transfers, decentralize marketing of decentralized autonomous organizations, ensure data quality through anomaly detection, and create decision-making AI systems for organizations to determine factors like profit sharing. Overall, AI-backed smart contracts create dynamic and versatile contracts that can respond to events, while AI and blockchain integration broadly opens up new possibilities across industries including real estate, gaming, data analytics, and organizational management. The paper emphasizes the transformative potential of synthesizing AI, smart contracts, and blockchain to make processes more adaptive, secure, incentivized and optimized.

**Method**

The paper proposes integrating artificial intelligence into smart contracts to enhance monitoring, adaptability, and new functionality. It suggests using AI for real-time monitoring and attack alerts in smart contracts. A decentralized, incentivized AI approach is also proposed for blockchain marketing of businesses and organizations. For data analytics, the Isolation Forest ensemble model is utilized to detect anomalies in oracle datasets by isolating observations based on path lengths. A simulation implements this using scikit-learn's Isolation Forest to train an anomaly detection smart contract. Additionally, the paper mentions using Generative Adversarial Networks, which employ competing generator and discriminator networks, to generate new data. Overall, the proposed AI integration aims to overcome limitations and add capabilities like enhanced security, decentralized marketing, anomaly detection, and data generation to make smart contracts more robust, adaptive and useful in practice.

**Result**

The paper proposes integrating artificial intelligence into smart contracts to add capabilities like real-time monitoring, attack alerts, and decentralized incentivized marketing of blockchain businesses and organizations. For data analytics, the Isolation Forest anomaly detection model is utilized to identify irregularities in oracle datasets based on path lengths. A simulation implements this using scikit-learn's Isolation Forest to train an anomaly detection smart contract. The combination of AI and blockchain has the potential to increase blockchain adoption across industries. However, challenges remain around infrastructure, data access control, and blockchain standardization. Overall, the incorporation of AI aims to enhance smart contract functionality with adaptive intelligence for security, automation, optimization, and new applications. But realizing the full potential of AI-driven smart contracts on blockchain requires overcoming key technical and regulatory hurdles.

**Conclusion**

The paper advocates for integrating artificial intelligence into smart contracts to enhance functionality and overcome limitations. Incorporating AI enables real-time monitoring and alerts for attacks on smart contracts. AI can also decentralize and incentivize blockchain marketing for businesses and organizations. For data analytics, the Isolation Forest model detects anomalies in oracle datasets. The combination of AI and blockchain has potential to increase blockchain adoption across industries. However, challenges remain around infrastructure, regulated data access, and lack of blockchain standards. Overall, the paper argues AI-driven smart contracts create more adaptive, secure and optimized contracts while AI-blockchain integration unlocks new possibilities. But technical and regulatory hurdles must be overcome to fully realize the benefits of converging these technologies.

**Future work**

The paper proposes several promising directions for further research on integrating AI and smart contracts. Additional exploration of applications in other industries and domains beyond the outlined use cases would be beneficial. More studies assessing the feasibility and obstacles around training AI models directly on the blockchain are needed. Developing supporting frameworks and infrastructure to address key issues like access control, privacy, and standardization is another critical area for future work. Specific to anomaly detection, further research could optimize the performance and efficiency of the Isolation Forest model for smart contracts, as well as investigate other AI techniques. Overall, the suggested future work aims to expand the understanding and methods for converging AI and blockchain through studying real-world applications, infrastructure requirements, on-chain model training, and refining analytical techniques like anomaly detection algorithms. Advancing these research areas will unlock the full potential of AI-driven smart contracts.

**Smart Contract Generation Assisted by AI-based word Segmentation**

**Abstract**

The paper proposes an AI-assisted Smart Contract Generation (AIASCG) framework to facilitate collaborative negotiation and drafting of contract clauses in natural language, bridging the gap between smart contracts and legal contracts. The framework adopts Machine Natural Language (MNL) as a universal representation and introduces an AI technique called Separation Inference (SpIn) to automatically segment sentences into semantically meaningful words, reducing manual effort. SpIn achieves high accuracy by inferring separations between words based on linguistic conventions. By generating smart contracts from negotiated clauses in MNL, the AIASCG framework creates legally enforceable smart contracts aligned with natural language agreements. This improves compatibility between blockchain and traditional contracts while leveraging AI to automate parts of the generation process. Overall, the AIASCG framework aims to combine the benefits of blockchain smart contracts and natural language legal contracts using AI-driven automation.

**Method**

The paper proposes an AI-assisted smart contract generation framework enabling collaborative drafting of natural language clauses which are converted to smart contracts. A key technique is Separation Inference (SpIn) - an AI approach to automatically split sentences into meaningful words, evaluated on multiple datasets with state-of-the-art accuracy and recall. Human assessment validates it can eliminate 80-100% of manual effort for 88% of sentences. Unlike typical word segmentation relying on contextual knowledge, SpIn refines the task as finding separations between words based only on bigrams, replacing complex CRF networks with softmax classification. This context-free approach directly segments sentences without tracking state transitions. By combining natural language negotiation with AI-driven drafting automation, the framework aims to bridge the gap between legal contracts and blockchain smart contracts for improved compatibility and efficiency.

**Result**

he proposed AIASCG framework with the SpIn technique demonstrates high effectiveness and efficiency for contract generation. SpIn achieves state-of-the-art F1 and recall across multiple word segmentation datasets in four languages, with human evaluation validating up to 100% time savings for 88% of sentences. This universal approach addresses incompatibility between smart contracts and legal contracts by enabling collaborative drafting of natural language clauses converted to machine natural language smart contracts. By automating semantic word splitting, the framework significantly reduces manual effort for generation. SpIn's simplified architecture deviates from complex networks and n-grams to deliver accurate, language-agnostic word segmentation. Overall, AIASCG combines natural language agreements with AI automation to bridge the gap between blockchain and traditional contracts, while SpIn's novel segmentation technique offers an efficient way to extract meaning from sentences through robust cross-lingual performance.

**Conclusion**

The paper proposes an AI-assisted Smart Contract Generation (AIASCG) framework to enable collaborative negotiation and drafting of natural language contract clauses, improving compatibility between blockchain smart contracts and legal contracts. The core Separation Inference (SpIn) technique automates semantic word splitting to significantly reduce manual effort in contract generation. SpIn achieves state-of-the-art effectiveness and human satisfaction on multi-language word segmentation tasks. This language-agnostic approach demonstrates robust performance across Chinese, Japanese, Korean and Thai. By combining AI-assisted editing and automatic segmentation, the AIASCG framework offers a new method for efficient smart contract generation from negotiated clauses. The integration of natural language agreements and AI automation aims to increase efficiency and bridge the gap between traditional and blockchain contracts. Overall, the paper emphasizes using AI techniques like SpIn to extract meaning from natural language and convert negotiated clauses into machine-readable smart contracts.

**Future work**

The paper proposes several directions for future work to build on the AIASCG framework and SpIn technique. Enhancing compatibility with existing software and expanding SpIn's language coverage beyond Chinese, Japanese, Korean and Thai would improve versatility. Additional AI techniques could be explored to further optimize the contract drafting process. More extensive user evaluations are needed to validate effectiveness in reducing manual effort, improving quality, and enabling collaboration. Investigating integration with blockchain platforms and real-world applications in finance, law, supply chain, etc would demonstrate practical viability. Overall, the suggested future work aims to strengthen interoperability, language support, automation capabilities, usability testing, and real-world deployment of the AIASCG framework. Advancing these areas will maximize the framework's potential to bridge the gap between natural language and smart contract constructs through AI assistance.

**Automated Vulnerability Detection for Solana Smart Contracts**

**Abstract**

VRust is a tool that performs whole program static data flow analysis on Rust MIR to detect vulnerabilities in Solana smart contracts. It translates source code to MIR and builds novel inference rules leveraging MIR constructs and inter-procedural analysis. For each crate, VRust generates a PDF report listing all vulnerabilities identified, including type, location, functions, and call stacks. The report also provides descriptions of each vulnerability and potential mitigations. By constructing targeted inference rules based on Rust MIR semantics, and tracing data flows across functions, VRust is able to accurately pinpoint vulnerabilities and their propagation in Solana smart contracts. The output provides actionable insights to developers for alleviating security issues.

**Method**

The paper proposes VRust, a vulnerability detection framework for Solana smart contracts using static analysis rules to validate input accounts and Rust MIR-based inference without annotations. It checks eight vulnerability types fully automatically and generates per-crate PDF reports listing identified issues, types, locations, functions, and call stacks. VRust performs whole-program data flow analysis by constructing novel inference rules leveraging Rust MIR semantics and inter-procedural tracing. By translating source code to MIR and analyzing data flows, it can pinpoint vulnerabilities across functions and call stacks. The generated reports provide actionable details including vulnerable lines, descriptive summaries, and potential mitigations to help developers address security issues. Overall, VRust advances Solana security through its automated, annotation-free methodology using Rust MIR and data flow analysis to detect vulnerabilities and their propagation at the whole-program level.

**Result**

VRust has been evaluated on over 100 Solana projects, discovering 12 new vulnerabilities including 3 critical issues in the official Solana library confirmed by developers. It generates per-crate PDF reports listing found vulnerabilities, types, locations, functions, call stacks, descriptions and mitigations. Without needing annotations, VRust fully automatically checks for 8 vulnerability types. Detailed results are provided for 12 real-world projects totaling 146,861 lines of code, including statistics on vulnerabilities detected per checker. The tool revealed numerous previously unknown flaws, validated by developers, demonstrating its capability in identifying security issues. By leveraging Rust semantics and data flow analysis, VRust pinpoints precise vulnerability details across entire codebases to help developers remediate concerns early before contract deployment. The thorough evaluations on real projects showcase VRust's effectiveness at automatically detecting varied vulnerability types in Solana smart contracts.

**Conclusion**

The paper proposes VRust, a novel vulnerability detection framework for Solana smart contracts. VRust successfully discovered previously unknown critical vulnerabilities in the official Solana library, confirmed by developers. It uniquely leverages static analysis rules and Rust MIR-based inference without annotations to detect issues automatically. VRust generates detailed audition reports listing found vulnerabilities, types, locations, functions, and call stacks to inform remediation. Evaluated on over 100 projects, it has proven effective at identifying varied flaws, enhancing Solana security. By building targeted inference rules from source code semantics and translating to MIR, VRust can pinpoint vulnerabilities without manual effort. The tool's ability to reveal unknown critical bugs validates its capability to audit Solana contracts. Overall, VRust advances Solana smart contract security through its automated inference-based static analysis methodology that provides actionable details to address vulnerabilities.

**Future work**

The paper proposes several areas of future work to enhance VRust: automating proof-of-concept generation for vulnerabilities; improving alias analysis to handle inter-procedural relations and indirect calls; adding capabilities to address global variables; reducing false positives, especially for complex semantics; incorporating symbolic execution to bypass branches; and expanded large-scale evaluation on diverse Solana projects. Automated PoC generation and upgraded alias analysis would increase automation and precision. Handling global variables and refining detection would improve analysis accuracy. Symbolic execution integration can boost PoC automation. Broader evaluations will further validate and refine VRust's effectiveness. Overall, the suggested enhancements aim to increase automation, precision, code coverage, and applicability across projects to solidify VRust's capabilities for reliable, holistic vulnerability detection in Solana smart contracts.

**Strengthening the Security of Smart Contracts through the Power of Artificial Intelligence**

**Abstract**

The paper explores utilizing artificial intelligence (AI) to bolster security for blockchain-based smart contracts (SCs), which are vulnerable to attacks due to complexity and lack of standards. It provides background on SCs and blockchain, outlines potential SC attacks, introduces AI categories and cybersecurity applications, and analyzes how AI can enhance SC security. The research shows AI can effectively defend against SC attacks and improve security and reliability, establishing a foundation for further research. By overviewing the landscape of SCs, threats, and AI techniques, and demonstrating AI's capabilities in safeguarding SCs, the paper makes the case for further exploring AI to combat issues stemming from SC complexity and establish robust security assurances. This lays groundwork for advancing the intersection of AI and blockchain to harden SCs against emerging attacks through automated intelligence.

**Method**

The paper investigates utilizing artificial intelligence (AI) to improve smart contract (SC) security, providing an overview of SCs, blockchain, and potential attacks. It introduces different AI categories and cybersecurity applications, followed by in-depth analysis of how AI can enhance SC security. The paper highlights open questions and future directions, examining AI's advantages in identifying and stopping threats. It reviews unresolved challenges and areas for further study like the need for labeled SC vulnerability data. Additionally, it describes SCs and their security holes stemming from complexity and lack of standards. By surveying the landscape and demonstrating AI's potential, the paper lays the groundwork for further research on applying automated intelligence to address SC security issues through detection, prevention, and response to emerging attacks.

**Result**

The paper demonstrates that artificial intelligence (AI) can effectively defend against attacks on smart contracts (SCs) and enhance their security and reliability. It highlights AI's potential to identify and halt SC threats. However, the study emphasizes the need for further research, as challenges remain around limited data and possible adversarial attacks. While underscoring AI's capabilities in safeguarding SCs, the paper lays the groundwork for advancing the field by outlining open questions around model vulnerabilities, interpretability, and robustness. By providing a comprehensive analysis of how AI techniques such as machine learning, deep learning, and natural language processing can be applied to combat SC security issues, the research establishes a framework and direction for future inquiry into hardening SCs through automated intelligence. Overall, the paper makes a compelling case that AI holds promise for securing complex, standardized SCs against emerging threats if key research gaps can be addressed.

**Conclusion**

The paper proposes several areas for future research to advance AI-based security for smart contracts (SCs): Developing AI detection tools that scale to large breach data; comprehensive studies benchmarking AI vulnerability identification to serve as a research reference; and exploring SSL and RL which have potential to overcome supervised learning constraints. Building scalable AI systems would enable identifying threats in large SC datasets. Rigorous assessments of AI techniques can standardize evaluation and direct progress. Finally, shifting focus to SSL and RL may mitigate limitations of supervised methods relying on labeled data. Overall, the suggested research aims to realize AI's full capabilities in SC security through scalable systems, extensive benchmarks, and cutting-edge techniques like SSL and RL that reduce dependence on scarce labeled data. Pursuing these directions can unlock AI's capacity to reliably detect vulnerabilities in complex, ever-evolving SCs.

**Future work**

The paper proposes several research directions to advance AI for enhancing smart contract (SC) security: Developing scalable AI systems to detect breaches in large SC data; comprehensive benchmarking studies of AI-based vulnerability identification as a reference for future research; and exploring SSL and RL to mitigate limitations of supervised learning. Building AI tools to handle sizable SC data could enable identifying threats hidden in vast amounts of blockchain activity logs and transactions. Standardized assessments of AI techniques would provide baselines to guide progress. Shifting focus to SSL and RL reduces dependence on labeled training data. Overall, the suggested work aims to realize AI's full potential in SC security through scalable and rigorous systems leveraging SSL, RL and other cutting-edge methods less reliant on scarce supervised data. Advancing these areas will unlock AI's capacity to reliably detect exploits in complex, ever-evolving SCs at large scale.

**Cryptocurrencies, Smart Contracts and Artificial Intelligence**

**Abstract**

The paper discusses recent developments in cryptocurrencies like Bitcoin and smart contract platforms like Ethereum. It explains how they work technically and some of their social implications. The paper suggests that as these technologies interact more with the physical world and legal systems, integration with AI techniques would be beneficial. AI could help translate real world data into formats usable by smart contracts. Smart contracts may also help ensure AI systems follow laws and norms.

**Method**

The paper provides background information on cryptocurrencies and how the blockchain consensus mechanism allows decentralized digital currencies. It explains smart contracts as self-enforcing contractual agreements and how platforms like Ethereum support complex smart contracts. Several examples are given of potential applications integrating cryptocurrencies, smart contracts, the internet of things, distributed autonomous organizations, and legal systems.

**Results**

The paper argues that integrating AI with cryptocurrency and smart contract platforms will be mutually beneficial. AI can provide the reasoning and real world knowledge to translate sensor data into smart contract clauses. Smart contracts can provide a way to ensure AI systems follow societal laws and norms. Significant innovation in these areas is needed as they could impact many aspects of society.

**Conclusion**

In conclusion, cryptocurrencies and smart contracts are emerging technologies with far-reaching implications. As they interact more with the physical world, integration with AI would allow more sophisticated reasoning and autonomy while still ensuring ethical constraints. Much research is needed to realize the potential of these technologies to transform commerce, organizations, and governance.

**Future Work**

The author suggests these technologies may lead to a "distributed autonomous society", but many open research questions remain. Further work is needed in translating real world data into smart contract formats, creating AI systems to reason about and participate in decentralized organizations, ensuring AI obeys laws and ethics through cryptocurrency incentives, and innovating new applications of integrated AI, cryptocurrencies, and smart contracts. Legal, economic, and social challenges around these technologies also require ongoing research.

**Intelligent Contracts: Making smart contracts smart for blockchain intelligence**

**Abstract**

The paper proposes a framework for constructing and applying Intelligent Contracts (ICs), which are smart contracts designed for blockchain-based AI tasks. It formulates two modes to construct ICs: encoding AI models (Mode 1) and scheduling AI collaboration (Mode 2). Experiments implement and evaluate ICs for classifying IRIS, MNIST, and ImageNet datasets on Ethereum blockchain.

**Method**

The paper implements ICs on Ethereum using Solidity and evaluates their classification accuracy and gas costs. Mode 1 directly encodes classifiers like decision trees and neural networks into smart contracts executing on-chain. Mode 2 uses smart contracts to schedule off-chain AI model execution while performing verification on-chain. Experiments encode 4 classifiers for IRIS, and 3 classifiers for MNIST and ImageNet.

**Results**

Experiments show Mode 1 ICs achieve the same accuracy as original classifiers but have high gas costs. Mode 2 reduces gas costs by offloading computation off-chain but adds communication costs. Analysis provides guidance on selecting modes based on use case. Mode 1 suits transparency and security needs but is constrained by blockchain capabilities. Mode 2 supports complex models with lower on-chain costs but requires security considerations.

**Conclusion**

The paper demonstrates feasibility of constructing ICs using two modes with trade-offs. Mode 1 provides on-chain autonomy while Mode 2 enables complex models via off-chain computing. Systematic analysis and experiments provide insights on constructing and applying ICs for blockchain AI tasks. ICs are key to enabling decentralized AI and AI-driven blockchain intelligence.

**Future Work**

More research is needed on: improving blockchain computation to expand Mode 1; optimization of security, storage and communication costs for Mode 2; managing reusable modular ICs; and automatic configuration of ICs to enable blockchain intelligence. Legal and social impacts of applying ICs also require ongoing investigation.

**TAIRA-BSC - Trusting AI in Recruitment Applications through Blokchain Smart Contracts**

**Abstract**

The paper proposes integrating blockchain smart contracts with AI and data lake technologies for trustworthy job recruitment systems. It presents the design of TAIRA-BSC, a conceptual architecture using blockchain, smart contracts, machine learning and data lake. The system extracts information from candidate and job data to match vacancies with qualified candidates.

**Method**

The paper reviews state-of-the-art in blockchain, AI, and labor markets. It identifies opportunities to address issues like transparency and trust. The TAIRA-BSC architecture is proposed with four layers: data lake, initial screening, mapping, and preferences. Sequence diagrams specify system functions and interactions between stakeholders. Smart contracts would trigger events and execute procedures for recruitment tasks.

**Results**

The system architecture and sequence diagrams demonstrate feasibility of the approach. Smart contracts can generate pre-selection candidate lists matching job descriptions using AI and blockchain’s transparency and automation. The integration of technologies enhances trust, security, and efficiency in recruitment.

**Conclusion**

The conceptual architecture shows blockchain smart contracts combined with AI and data lake can revolutionize recruitment systems by bridging trust concerns. The system simplifies recruitment, protects sensitive data, and ensures integrity. Further research will involve implementing a proof-of-concept to evaluate the framework.

**Future Work**

Next steps include refining system goals with stakeholders, developing and testing components, and evaluating efficiency gains. Research on legal and social impacts of such decentralized systems is also needed. Optimizing security, storage, and communication costs are areas for improvement.

**Who is smarter? An empirical study of AI-based smart contract creation**

**Abstract**

The paper assesses code quality of smart contracts generated by large language models (LLMs) including ChatGPT and Google Palm2. It reveals evidence of security bugs and deficiencies in correctness. Additionally, the study identifies areas to enhance process, quality, and safety of automatically generated smart contract code. It suggests LLMs require improvement to avoid introducing vulnerabilities when drafting smart contracts through generative methods. By evaluating overall code quality as well as security-specific aspects, the research highlights risks with current LLMs' smart contract capabilities. It proposes future work to advance models' understanding of security best practices and improve the reliability of generated code. Altogether, the paper demonstrates gaps that pose threats when applying LLMs for automated smart contract generation, while pointing to research directions that can overcome these limitations.

**Method**

The paper proposes an experimental framework to evaluate code quality of smart contracts generated by large language models (LLMs). It assesses the method's effectiveness, scalability, and prompt transferability between models. Additionally, it demonstrates the approach can identify security vulnerabilities in code produced by GPT models. By establishing an evaluation pipeline, the study aims to benchmark LLMs' smart contract coding capabilities to guide improvements. The research reveals current limitations in correctness, security, and reliability of generated code. Testing prompt transferability also evaluates consistency across models. Overall, the proposed evaluation methodology enables systematically measuring LLMs' competency in drafting secure, high-quality smart contracts autonomously. The paper not only surfaces deficiencies posing risks if deployed, but also provides a testing framework to track progress of generative AI for safe, functional smart contract creation.

**Result**

The study revealed security bugs being introduced in smart contracts generated by large language models like ChatGPT and Google Palm2, impacting overall quality and correctness. The paper evaluated code validity, efficiency, and reliability using static analysis tools and MythX to categorize vulnerabilities based on severity. It identified areas for improvement in the generation process and proposed research directions to enhance quality and security. The experimental workflow assessed models on data preprocessing, code templates, compilation, and multiple quality dimensions including security, maintainability, and efficiency. By systematically evaluating generated code, the paper demonstrated risks posed by current model limitations and outlined a testing methodology to address gaps. Taken together, the findings underscore deficiencies in existing generative AI for secure smart contract creation while providing a framework to benchmark progress.

**Conclusion**

The study evaluated smart contract code generated by large language models (LLMs), finding both ChatGPT and Google Palm2 introduced security bugs, impacting overall quality and correctness. The paper proposed an automated validation framework to verify generated code. Template-based generation using context was better than prompts alone for producing compilable code. While Google Palm2 created more compilable code, both models exhibited similar bug rates, making recommendations difficult. The research identified enhancements needed in the generation process and suggested directions to improve quality and security of generated codes, including better comprehension of vulnerabilities. Overall, the study revealed deficiencies in existing LLMs' smart contract coding capabilities by systematically assessing model-produced code. The proposed pipeline enables tracking progress, while highlighting areas such as security knowledge integration to mature AI-based smart contract generation.

**Future work**

The paper proposes several promising research directions to improve process, quality, and security of smart contracts generated by large language models: Exploring prompt engineering techniques to enhance model code outputs; studying prompt transferability between models to understand scalability; developing prompt patterns that enforce constraints and provide context to improve problem-solving; conducting more research to mitigate introduced security bugs; refining the experimental and validation framework to automate verification. Advancing prompting methodologies and transferability assessments could increase effectiveness and consistency of generated codes. Enhanced prompt engineering and security research can reduce risks and errors. Automating the pipeline would enable systematic testing. Overall, the suggested areas aim to mature model capabilities, prompt design, and evaluative frameworks to realize greater reliability, quality and safety for AI-generated smart contracts.

**Intelligent Smart Contracts for Innovative Supply Chain Management**

**Abstract**

The paper proposes the use of blockchains and smart contracts for innovative supply chain management to achieve higher levels of collaboration between companies participating in the chain. The smart contracts aim to solve the problems of trust and coordination, replacing human coordinators and automating the process of coordination, thus unburdening the supply chain of considerable management costs.

**Method**

The paper proposes the use of blockchains and smart contracts for innovative supply chain management. It introduces a type of smart contract aimed to solve the problems of trust and coordination in supply chains. The paper details the algorithmic methodologies underlying the decision-making process of these contracts and outlines the wider socio-economic perspectives opened by their approach. However, the paper does not mention any specific methods used in the research.

**Result**

The paper does not provide any specific results as it is a proposal for the use of blockchains and smart contracts for innovative supply chain management. It outlines the potential benefits of using intelligent smart contracts to solve the problems of trust and coordination in supply chains, replacing human coordinators and automating the process of coordination, thus unburdening the supply chain of considerable management costs.

**Conclusion**

The paper proposes the use of blockchains and smart contracts for innovative supply chain management, introducing the concept of Intelligent Smart Contract, which is characterized not only by "smartness" but also by "intelligence." The paper outlines the potential benefits of using intelligent smart contracts to solve the problems of trust and coordination in supply chains, replacing human coordinators and automating the process of coordination, thus unburdening the supply chain of considerable management costs. The paper provides an instance of an intelligent smart contract, both from an algorithmic and an architectural standpoint, as given by Revenue Sharing, a methodology for supply chain management that can greatly boost the profitability of the supply chain for the benefit of all participants. The paper concludes that intelligent smart contracts running on blockchain can achieve higher levels of collaboration between the companies participating in the chain, resulting in higher levels of profitability and economic health for the participating enterprises.

**Future work**

The paper suggests future work along two lines, one technological and the other organizational. The technological line of future work involves the development of more advanced algorithms for intelligent smart contracts, which can take into account more complex scenarios and decision-making processes. The organizational line of future work involves the implementation of intelligent smart contracts in real-world supply chains, testing their effectiveness and scalability. The paper also suggests that the proposed approach can be evaluated within a wider evaluation grid, which includes not just the improvements in transaction costs deriving from the systematic adoption of digital trust made available by the blockchain, but also the optimal management of resources as implemented in the intelligent smart contract of Revenue Sharing, as well as the possibility of dynamically creating new supply agreements between partners that may lack former business relationships.

**VRust: Automated Vulnerability Detection for Solana Smart Contracts**

**Abstract**

The paper proposes VRust, an automated smart contract vulnerability detection framework for Solana. It uses static analysis rules to validate untrustful input accounts and can detect eight different vulnerability types without any code annotations.

**Method**

The paper proposes VRust, an automated smart contract vulnerability detection framework for Solana. It uses static analysis rules to validate untrustful input accounts and can detect eight different vulnerability types without any code annotations. The key technical novelty is a set of static analysis rules for validating untrustful input accounts that are unique in the Solana programming model. The source code is translated into Rust MIR-based inference rules to check all the vulnerabilities fully automatically. VRust has been evaluated on over a hundred of Solana projects, and it has revealed 12 previously unknown vulnerabilities, including 3 critical vulnerabilities in the official Solana Programming Library confirmed by core developers.

**Result**

The paper evaluated the VRust framework on over one hundred Solana smart contracts, and provided detailed results for 12 popular real-world projects with 146,861 LoC. It collected the statistics on 12 projects for the number of vulnerabilities reported for each checker. VRust was able to detect 12 previously unknown vulnerabilities, including 3 critical vulnerabilities in the official Solana Programming Library confirmed by core developers. The paper also discusses the soundness and completeness of VRust and the main reasons for false positives.

**Conclusion**

The paper proposes VRust, the first automated smart contract vulnerability detection framework for Solana. It can detect eight different vulnerability types without any code annotations and has been evaluated on over a hundred of Solana projects, revealing 12 previously unknown vulnerabilities, including 3 critical vulnerabilities in the official Solana Programming Library confirmed by core developers. The paper concludes that VRust is an end-to-end vulnerability detector for Solana smart contracts that can produce detailed vulnerability audition reports and has the potential to improve the security of Solana smart contracts.

**Future work**

The paper suggests several future works that can be done to improve the VRust framework and the security of Solana smart contracts. Some of the future works suggested in the paper are:

* Improving the precision of the VRust framework by incorporating more advanced techniques such as symbolic execution and model checking.
* Developing a more comprehensive set of vulnerability types to detect more complex vulnerabilities in Solana smart contracts.
* Integrating VRust into the Solana development environment to provide developers with real-time feedback on potential vulnerabilities.
* Investigating the effectiveness of VRust on other blockchain platforms and smart contract languages.
* Developing a tool to automatically fix the detected vulnerabilities in Solana smart contracts.

These future works can help improve the security of Solana smart contracts and make the development process more efficient and secure.

**Blockchain Smart Contract to Prevent Forgery of Degree Certificates: Artificial Intelligence Consensus Algorithm**

**Abstract**

The paper proposes the use of a Blockchain-based diploma to prevent forgery of degree certificates. It also suggests the use of an artificial intelligence consensus algorithm and natural language processing for verification work.

**Method**

The paper proposes the use of a Blockchain-based diploma to prevent forgery of degree certificates. It uses an automatic translation system that incorporates natural language processing to perform verification work that does not require an existing public certificate. The hash algorithm is used to authenticate security. The paper also suggests the use of an artificial intelligence consensus algorithm for verification work. The methodology uses a neuron engine and Blockchain to accurately record the graduates' academic records without falsifying them. The paper provides an experimental environment with at least 10 nodes constructed, and a platform test, measurement test, and performance measurement test are conducted to assess the smart contract development and performance measurement.

**Result**

a Blockchain-based diploma file. The analysis of the artificial intelligence distribution diagram was conducted using a four-point method, and the distribution chart was evenly distributed, confirming the diploma with the highest similarity. The verified values were then analyzed. The paper proposes natural language processing-based Blockchain algorithms.

**Conclusion**

The paper concludes that a Blockchain-based diploma can be used to prevent forgery of degree certificates. The proposed methodology uses an automatic translation system that incorporates natural language processing and an artificial intelligence consensus algorithm for verification work. The paper suggests that these security protocols can provide more secure data protection. The experimental environment with at least 10 nodes constructed, and a platform test, measurement test, and performance measurement test are conducted to assess the smart contract development and performance measurement. The paper proposes natural language processing-based Blockchain algorithms.

**Future work**

The paper suggests that in the future, mechanisms should be studied to verify the first Genesis block, and an artificial intelligence blockchain-based graduation certificate system should be studied from the perspective of OSI 7 Layer, including network security, server security, and intercept security until the original image is registered in the original node. The paper also suggests that more tests should be conducted on more users to supplement the collected usage data. Additionally, the paper proposes that services using Blockchain platforms should be verified through development and testing in other environments in the future.

**Strengthening the Security of Smart Contracts through the Power of Artificial Intelligence**

**Abstract**

The paper investigates the use of artificial intelligence (AI) to improve the security of smart contracts (SCs) stored on a blockchain. The authors provide an overview of SCs and blockchain technology, discuss possible SC-based attacks, and analyze how AI can be used to enhance SC security.

**Method**

The paper investigates the use of artificial intelligence (AI) to improve the security of smart contracts (SCs) stored on a blockchain. The authors provide an overview of SCs and blockchain technology, discuss possible SC-based attacks, and analyze how AI can be used to enhance SC security. The methods used in this paper include:

* Providing an overview of Smart Contracts (SCs) and blockchain technology
* Discussing possible SC-based attacks
* Introducing various AI categories and their applications in cybersecurity
* Analyzing how AI can be used to enhance SC security
* Highlighting open questions and future directions of research in this field.

**Result**

The paper aims to investigate the use of artificial intelligence (AI) to improve the security of smart contracts (SCs) stored on a blockchain. The authors provide an overview of SCs and blockchain technology, discuss possible SC-based attacks, and analyze how AI can be used to enhance SC security. The paper concludes that AI can provide an effective defense against assaults on SCs and contribute to their security and dependability. The article lays the groundwork for future research in the field of AI for SC security. Therefore, the results of the paper suggest that AI can be used to enhance the security of smart contracts.

**Conclusion**

The paper concludes that AI can provide an effective defense against assaults on smart contracts (SCs) and contribute to their security and dependability. The authors suggest that AI can be used to enhance the security of SCs and lay the groundwork for future research in the field of AI for SC security.

**Future work**

The paper suggests that future research in the field of smart contracts (SCs) and artificial intelligence (AI) should focus on the following:

* Creation of AI-powered detection tools for SC-related security breaches that can handle ever-increasing amounts of data.
* Comprehensive study into SC flaw detection using AI, which can serve as both a point of reference and a source of ideas for future research.
* Giving more attention to SSL and RL, which have the potential to overcome the constraints of SL.
* Integration of AI with formal techniques to achieve a more rigorous and comprehensive security research of SCs.

These suggestions can help improve the security and dependability of SCs and pave the way for further advancements in the field of AI for SC security.

**Intelligent contracts: Making smart contracts smart for blockchain intelligence**

**Abstract**

The paper proposes a framework for constructing and applying Intelligent Contracts (ICs) for blockchain-based AI tasks. ICs are special Smart Contracts designed for tasks requiring intelligence, and the framework includes two construction modes and a technical route for optimal configuration and automatic response.

**Method**

The paper proposes a constructive framework for Intelligent Contracts (ICs) and conducts a systematic analysis. The methods used in this paper are as follows:

Review of related work in blockchain, Smart Contracts, distributed AI, and crossover research on blockchain and AI.

Formulation of two construction modes of ICs, including encoding AI models and scheduling AI collaboration.

Comparison of the characteristics of these two modes theoretically and experimentally.

Proposal of a technical route for optimal configuration and automatic response of ICs to encourage AI-driven blockchain intelligence.

Implementation and thorough evaluation of two modes of ICs on Ethereum using typical AI tasks of classifying IRIS, MNIST, and ImageNet data sets as examples.

Illustration of the optimal configuration and automatic response process of ICs based on the constructed ICs in experiments.

Overall, the paper uses a combination of theoretical analysis, experimental evaluation, and proposal of a technical route to demonstrate the effectiveness and feasibility of the proposed framework for ICs.

**Result**

The paper demonstrates the effectiveness and feasibility of the proposed framework for Intelligent Contracts (ICs) through implementation and thorough evaluation of two modes of ICs on Ethereum using typical AI tasks of classifying IRIS, MNIST, and ImageNet data sets as examples. The experimental results show that the proposed framework is effective in achieving AI-driven blockchain intelligence and can be used to construct and apply ICs for blockchain-based AI tasks.

**Conclusion**

The conclusion of the paper is that Intelligent Contracts (ICs) are an important type of Smart Contracts (SCs) designed to accomplish blockchain-based AI tasks. The paper proposes a constructive framework for the construction and application of ICs, which includes two modes: encoding AI models and scheduling AI collaboration. The paper also proposes a technical route for optimal configuration and automatic response of ICs to encourage AI-driven blockchain intelligence. The experimental results demonstrate the effectiveness and feasibility of the proposed framework. Overall, the paper provides a systematic analysis of ICs and a constructive framework for their construction and application, which can be used to achieve AI-driven blockchain intelligence.

**Future work**

The paper suggests several future works related to Intelligent Contracts (ICs) and their application in blockchain-based AI tasks. These include:

* Further research on the construction and application of ICs, including the development of new construction modes and the exploration of new application scenarios.
* Investigation of the security, privacy, and legal issues related to ICs and their application in blockchain-based AI tasks.
* Development of a decentralized market for modular and reusable ICs and associated AI collaboration modules to facilitate the sharing and exchange of ICs among different blockchain networks.
* Integration of ICs with other emerging technologies, such as edge computing and 5G networks, to enable more efficient and intelligent blockchain-based AI tasks.

These future works can help to further advance the field of blockchain-based AI and promote the development of AI-driven blockchain intelligence.

**Learning Markets: An AI Collaboration Framework Based on Blockchain and Smart Contracts**

**Abstract**

The paper proposes a decentralized AI collaboration framework called Learning Markets (LM) based on blockchain and smart contracts. LM provides a trustless environment for collaboration and transaction, while smart contracts serve as software-defined agents to encapsulate and process scalable collaboration relationships and market mechanisms.

**Method**

The paper proposes a decentralized AI collaboration framework called Learning Markets (LM) based on blockchain and smart contracts. The authors introduce the background that motivates LM, formulate the framework for related application requirements, elaborate its operation mechanisms and the detailed design of smart contracts, and compare their work with existing works. They also implement and comprehensively analyze LM based on the Ethereum interplenary file system platform (IPFS), and the results prove that it has advantages in collaboration fairness, transparency, security, decentralization, and universality. The paper uses a collaborative scenario for MNIST image classification task to comprehensively test the functions of smart contracts and evaluate and analyze the framework from multiple quantitative and nonquantitative indicators. The authors develop five smart contracts, i.e., AMSC, DTSC, MVSC, CESC, and IQSC, to implement and examine the proposed framework.

**Result**

The paper implements and comprehensively analyzes the Learning Markets (LM) framework based on the Ethereum interplenary file system platform (IPFS). The results show that LM has advantages in collaboration fairness, transparency, security, decentralization, and universality. The authors use a collaborative scenario for MNIST image classification task to comprehensively test the functions of smart contracts and evaluate and analyze the framework from multiple quantitative and nonquantitative indicators. The authors develop five smart contracts, i.e., AMSC, DTSC, MVSC, CESC, and IQSC, to implement and examine the proposed framework.

**Conclusion**

The paper proposes a novel decentralized AI collaboration framework called Learning Markets (LM) based on blockchain and smart contracts. The LM framework can help participants without mutual trust realize collaborative mining with dynamic and quantitative rewards and build an AI market with natural auditability and traceability for trading trusted and verified models. The LM framework has advantages in collaboration fairness, transparency, security, decentralization, and universality. The authors implement and comprehensively analyze LM based on the Ethereum interplenary file system platform (IPFS), and the results prove that it is a promising solution for distributed AI collaboration in data, models, and resources.

**Future work**

The paper suggests three future directions for research:

* Building standardized smart contracts that encapsulate intelligent algorithms or collaboration relationships to expand collaboration modes and promote technology sharing.
* Forming trusted static or dynamic intelligent component libraries that are easy to configure and reuse.
* Introducing special arbitration roles and smart contracts to deal with malicious behaviors that cannot be automatically verified.

**Leveraging ChatGPT for Automated Smart Contract Repair: A Preliminary Exploration of GPT-3-based Approaches**

**Abstract**

The paper proposes a novel approach for automatically repairing Solidity smart contracts using a large-scale language model called ChatGPT. The approach aims to detect and fix vulnerabilities in the code, ultimately improving the security and robustness of smart contract systems.

**Method**

The paper uses ChatGPT, a large-scale language model, to automatically repair Solidity smart contracts by training it through prompt engineering techniques, tailoring its capabilities to detect and fix vulnerabilities in the code. The performance of ChatGPT in smart contract Automatic Program Repair (APR) is evaluated using a dataset from previous research, combining SmartCorpus and SmartBugs. To identify vulnerabilities, diagnostic tools like HoneyBadger, Osiris, Oyente, Mythril, Slither, and Securify are used. Osiris focuses on detecting arithmetic bugs, reentrancy, improper uses of the call function, and time manipulation bugs. HoneyBadger identifies honeypots, while Oyente targets a limited subset of vulnerabilities.

**Result**

The paper presents the results of three experiments to evaluate ChatGPT's performance in repairing smart contracts. The initial dataset comprised 200 vulnerable contracts, reduced to 106 due to ChatGPT's size constraints. The reported vulnerabilities included 59 reentrancy instances, 181 arithmetic overflows/underflows, 28 time dependency bugs, and 43 unchecked low-level calls. The ChatGPT-based approach successfully repaired vulnerable Solidity smart contracts, and the returned smart contract is considered valid if all reported vulnerabilities are fixed, and the contract compiles. An incorrect response includes uncorrected code lines, partial fixes, non-compilable contracts, or altered pragma versions. The results showcase the potential of ChatGPT as a valuable tool for improving the security and robustness of smart contract systems in various use cases, ultimately reducing the risks associated with bugs and honeypots.

**Conclusion**

The paper concludes that ChatGPT is best utilized as an Automatic Program Repair (APR) tool when combined with vulnerability detection tools. The most effective approach involved inputting the vulnerable code snippet, exposed code lines, and associated vulnerabilities, achieving 89% accuracy. However, ChatGPT struggles with complex contracts and has limitations in analyzing large programs. Future work aims to expand the smart contract subset, include additional vulnerabilities (e.g., Denial of Service and front-running attacks), and leverage models like OpenAI Codex for automation. The dataset will be made open source to facilitate further research.

**Future work**

The paper suggests several future works, including:

* Expanding the smart contract subset to include additional vulnerabilities such as Denial of Service and front-running attacks.
* Leveraging models like OpenAI Codex for automation.
* Making the dataset open source to facilitate further research.

**Making Smart Contracts Smarter**

**Abstract**

The paper investigates the security of running smart contracts based on Ethereum in an open distributed network like those of cryptocurrencies. It introduces several new security problems in which an adversary can manipulate smart contract execution to gain profit and proposes ways to enhance the operational semantics of Ethereum to make contracts less vulnerable.

**Method**

The paper documents several new classes of security bugs in Ethereum smart contracts, formalizes the semantics of Ethereum smart contracts, and proposes recommendations as solutions for the documented bugs. It introduces a symbolic execution tool called Oyente to find potential security bugs in existing Ethereum contracts. The tool flags 8,833 of them as vulnerable, including the TheDAO bug which led to a 60 million US dollar loss in June 2016. The paper also discusses the severity of other attacks for several case studies which have source code available and confirms the attacks in the main Ethereum network.

**Result**

The paper flags 8,833 existing Ethereum contracts as vulnerable, including the TheDAO bug which led to a 60 million US dollar loss in June 2016. It also documents several new classes of security bugs in Ethereum smart contracts and proposes recommendations as solutions for the documented bugs. The paper introduces a symbolic execution tool called Oyente to find potential security bugs in existing Ethereum contracts. It also discusses the severity of other attacks for several case studies which have source code available and confirms the attacks in the main Ethereum network.

**Conclusion**

The paper concludes that the security of running smart contracts based on Ethereum in an open distributed network like those of cryptocurrencies is vulnerable to several new classes of security bugs. The proposed recommendations can enhance the operational semantics of Ethereum to make contracts less vulnerable. The symbolic execution tool called Oyente can be used by developers to find potential security bugs in existing Ethereum contracts. The severity of other attacks for several case studies which have source code available is also discussed in the paper.

**Future work**

The paper suggests several future works to enhance the security of smart contracts based on Ethereum. Some of the future works suggested in the paper are:

* Developing a more precise and efficient symbolic execution tool to detect security bugs in smart contracts.
* Developing a formal verification tool to prove the correctness of smart contracts.
* Developing a tool to automatically repair security bugs in smart contracts.
* Developing a tool to monitor the execution of smart contracts in real-time and detect anomalous behavior.
* Developing a tool to automatically generate test cases for smart contracts.
* Developing a tool to analyze the gas consumption of smart contracts and optimize their performance.

**Meet my artificially-intelligent virtual self: creative avatars, machine learning, smart contracts and the copyright conundrum**

**Abstract**

The abstract of the paper refers to a previous article by McCutcheon, which discusses the need for copyright policy to adapt to the computer age. It also cites three legal cases related to copyright and intellectual property.

**Method**

The paper does not provide information about the methods used. It is a commentary article that discusses the challenges of regulating rights in AI-generated derivative content and the need for copyright policy to adapt to the computer age.

**Result**

The paper is a commentary article that discusses the challenges of regulating rights in AI-generated derivative content and the need for copyright policy to adapt to the computer age. It does not present any specific results or findings.

**Conclusion**

The paper concludes that the development of intelligent AI applications that replicate the style of human authors poses regulatory challenges for copyright policy. The authors argue that copyright law needs to adapt to the computer age to address these challenges and ensure that the major objectives of copyright policy are satisfied. The paper highlights the need for a balanced approach that considers the interests of both creators and users of AI-generated content.

**Future work**

The paper does not suggest any specific future works. It is a commentary article that discusses the challenges of regulating rights in AI-generated derivative content and the need for copyright policy to adapt to the computer age.

**Privacy-preserving in smart contracts using blockchain and artificial intelligence for cyber risk measurements**

**Abstract**

The paper proposes a framework called Privacy-preserving in Smart Contracts using Blockchain and Artificial Intelligence (PPSC-BCAI) to simplify human interaction, system activities, service alerts, security risks, and fraudulent claims. The framework uses blockchain and AI to analyze data transactions and sharing, and an extreme gradient boosting (XGBoost) to optimize the network load.

**Method**

The paper proposes a framework called Privacy-preserving in Smart Contracts using Blockchain and Artificial Intelligence (PPSC-BCAI) to simplify human interaction, system activities, service alerts, security risks, and fraudulent claims. The framework uses blockchain and AI to analyze data transactions and sharing, and an extreme gradient boosting (XGBoost) to optimize the network load. The proposed framework includes training, validating, and testing the dataset obtained from an insurance company. The XGBoost algorithm is used to compute the accuracy of the key attributes that evaluate the performance model. The mean absolute error (MAE) is used to express the accuracy of the model.

**Result**

The paper does not provide a detailed discussion of the results obtained from the proposed framework. However, it mentions that the proposed framework is effective in simplifying human interaction, system activities, service alerts, security risks, and fraudulent claims. The framework uses blockchain and AI to analyze data transactions and sharing, and an extreme gradient boosting (XGBoost) to optimize the network load. The proposed framework includes training, validating, and testing the dataset obtained from an insurance company. The XGBoost algorithm is used to compute the accuracy of the key attributes that evaluate the performance model. The mean absolute error (MAE) is used to express the accuracy of the model.

**Conclusion**

The paper proposes a Privacy-preserving in Smart Contracts using Blockchain and Artificial Intelligence (PPSC-BCAI) framework to simplify human interaction, system activities, service alerts, security risks, and fraudulent claims. The proposed framework uses blockchain and AI to analyze data transactions and sharing, and an extreme gradient boosting (XGBoost) to optimize the network load. The paper concludes that the proposed framework is effective in improving system efficiencies and claims better efficiency than other existing schemes.

**Future work**

The paper suggests that in the future, the proposed PPSC-BCAI framework will be analyzed more realistically to classify the normalized confusion matrix and accuracy factors. However, the paper does not provide any further details on the future works.

**Self-Aware Smart Contracts with Legal Relevance**

**Abstract**

The paper proposes the use of self-aware contracts (SAC) that are machine-readable and supported by blockchain technology to address the challenges of conventional contracts (CC). SACs do not require qualitative trust between contracting parties and can be enforced through software agents. The paper presents a SAC framework for a decentralized peer-to-peer economy.

**Method**

The paper proposes a SAC framework for a decentralized peer-to-peer economy that is supported by blockchain technology and multi-agent systems. The authors use the Protégé tool, a free, open-source ontology editor, to design the ontology for the paper. They also employ the Her-miT reasoner to check the ontology consistency and identify subsumption relationships between classes. The paper specifies machine-readable obligation-and rights constructs for execution and enforcement. Additionally, the authors use a renting case to explain the business context provisions that comprise obligations and rights assigned to concrete process tasks.

**Result**

The paper presents a SAC framework that enables blockchain-driven self-aware agents-assisted contracts for a decentralized peer-to-peer economy. The proposed framework addresses the gap in current machine-readable contract solutions by specifying suitable obligation-and rights constructs for execution and enforcement. The authors use a renting case to explain the business context provisions that comprise obligations and rights assigned to concrete process tasks. The paper evaluates the results of the research and concludes with a future-work presentation.

**Conclusion**

The paper presents a novel cross-organizational blockchain-agnostic framework for peer-to-peer collaboration. The proposed SAC framework enables blockchain-driven self-aware agents-assisted contracts for a decentralized peer-to-peer economy. The authors use a renting case to explain the business context provisions that comprise obligations and rights assigned to concrete process tasks. The paper concludes that the proposed SAC framework addresses the gap in current machine-readable contract solutions by specifying suitable obligation-and rights constructs for execution and enforcement. The authors also present future work that includes the implementation of the SAC framework and the evaluation of its performance.

**Future work**

The paper suggests future work that includes the development of a mapping from SEC-Language obligations and rights to lower-level smart contract languages such as Solidity that operate directly on blockchain platforms. The authors also propose the implementation of the SAC framework and the evaluation of its performance.

**Smart Contract Generation Assisted by AI-Based Word Segmentation**

**Abstract**

The paper proposes an AI-assisted Smart Contract Generation (AIASCG) framework that allows contracting parties in different languages to collaboratively negotiate and draft the contract clauses. The framework uses an AI-based automatic word segmentation technique called Separation Inference (SpIn) to fulfill automatic split of the sentence, reducing the manual effort in contract generation.

**Method**

The paper proposes an AI-assisted Smart Contract Generation (AIASCG) framework that allows contracting parties in different languages to collaboratively negotiate and draft the contract clauses. The framework uses an AI-based automatic word segmentation technique called Separation Inference (SpIn) to fulfill automatic split of the sentence, reducing the manual effort in contract generation. The paper compares the design of AIASCG with existing smart contract generation approaches to present its novelty. The SpIn technique is evaluated from a robustness and human satisfaction point of view to demonstrate its effectiveness. In the robustness evaluation, SpIn achieves state-of-the-art F1 scores and Recall of Out-of-Vocabulary (R\_OOV) words on multiple word segmentation tasks. In addition, in the human evaluation, participants believe that 88.67% of sentences can be saved 80-100% of the time through automatic word segmentation. The paper introduces the differences in the mechanism between the proposed SpIn and existing WS algorithms. Existing WS methods consider WS as the sequence labeling task and introduce various tagging schemas. Although researchers tried to investigate rich context features or complex network structure to achieve better WS, they all based their research on the tagging schema. Regardless of the different tagging schemas applied, each tag indicates the position of the current character in a segment. Therefore, the implied information restricts the tag-to-tag transition, requiring CRF or rich contexts information to handle inaccurate tag transitions.

**Result**

The paper evaluates the proposed Separation Inference (SpIn) technique from a robustness and human satisfaction point of view to demonstrate its effectiveness. In the robustness evaluation, SpIn achieves state-of-the-art F1 scores and Recall of Out-of-Vocabulary (R\_OOV) words on multiple word segmentation tasks. In addition, in the human evaluation, participants believe that 88.67% of sentences can be saved 80-100% of the time through automatic word segmentation. The paper also introduces the differences in the mechanism between the proposed SpIn and existing WS algorithms. Existing WS methods consider WS as the sequence labeling task and introduce various tagging schemas.

**Conclusion**

The paper proposes an AI-assisted Smart Contract Generation (AIASCG) framework that allows contracting parties in different languages to collaboratively negotiate and draft the contract clauses. The framework uses an AI-based automatic word segmentation technique called Separation Inference (SpIn) to fulfill automatic split of the sentence, reducing the manual effort in contract generation. The SpIn technique is evaluated from a robustness and human satisfaction point of view to demonstrate its effectiveness. In the robustness evaluation, SpIn achieves state-of-the-art F1 scores and Recall of Out-of-Vocabulary (R\_OOV) words on multiple word segmentation tasks. In addition, in the human evaluation, participants believe that 88.67% of sentences can be saved 80-100% of the time through automatic word segmentation. The paper concludes that the proposed AIASCG framework with SpIn technique can address the issue of manual effort in contract generation and can extend the blockchain ecosystem and inspire next-era business paradigms.

**Future work**

The paper suggests two directions for future work on the proposed AIASCG framework.

* Interoperability of SIM: The current implementation of SIM in the paper has not been actively maintained, so its compatibility with existing software may be unsatisfying. Therefore, future work can focus on improving the interoperability of SIM with existing software.
* Completeness of SpIn language support: The SpIn technique proposed in the paper can be trained on the corpus in other languages to be more versatile. Therefore, future work can focus on improving the completeness of SpIn language support.

**Smart Contract Privacy Protection using AI in Cyber-Physical Systems: Tools, Techniques and Challenges**

**Abstract**

The paper discusses the challenges related to security and privacy in smart contracts (SCs) and explores various Artificial Intelligence (AI) techniques and tools for SC privacy protection. It also presents a case study of retail marketing that uses AI and SC to preserve its security and privacy.

**Method**

The paper is a survey-based research that identifies research questions from existing literature in the same area. It analyzes various Artificial Intelligence (AI) techniques and tools for smart contract (SC) privacy protection and presents a case study of retail marketing that uses AI and SC to preserve its security and privacy. Therefore, the methods used in this paper are literature review and case study analysis.

**Result**

The paper presents a survey on smart contract (SC) security vulnerabilities in the software code that can be easily hacked by a malicious user or may compromise the entire blockchain network. It also explores various Artificial Intelligence (AI) techniques and tools for SC privacy protection and presents a case study of retail marketing that uses AI and SC to preserve its security and privacy. The paper concludes that AI-based solutions can address security, privacy, and computation issues in SC applications.

**Conclusion**

The paper concludes that smart contracts (SCs) are modernizing the traditional industrial, technical, and business processes by eliminating the need for trusted third-party systems, which ultimately saves administration as well as service costs. However, SCs are vulnerable to security and privacy issues, and designing complex SCs cannot mitigate these issues. Therefore, the paper investigates various Artificial Intelligence (AI) techniques and tools for SC privacy protection and presents a case study of retail marketing that uses AI and SC to preserve its security and privacy. The paper suggests that AI-based solutions can address security, privacy, and computation issues in SC applications.

**Future work**

The paper suggests that future research can focus on the following areas related to smart contract (SC) security and privacy:

* Developing AI-based solutions for SCs that can address security, privacy, and computation issues.
* Investigating the use of AI techniques such as machine learning, deep learning, and natural language processing for SC privacy protection.
* Developing tools and techniques for detecting and mitigating SC vulnerabilities in the software code that can be easily hacked by a malicious user or may compromise the entire blockchain network.
* Analyzing the impact of SC complexity on energy efficiency, especially for low-powered IoT devices.
* Conducting more case studies to demonstrate the effectiveness of AI-based solutions for SC privacy protection in different domains.

Overall, the paper suggests that AI can play a significant role in addressing the security and privacy challenges of SCs, and future research can focus on developing more effective AI-based solutions for SC applications.

**Toward a self-learned Smart Contracts**

**Abstract**

The paper discusses the integration of Artificial Intelligence with Blockchain and how it can be used for forecasting and automating, building a self-regulated chain. It also highlights the lack of standardization in Blockchain architecture and the importance of considering smart contract costs, transaction fees, and storage on/off-chain.

**Method**

The paper does not explicitly mention any specific methods used. However, it discusses the main factors that affect the integration of Artificial Intelligence with Blockchain and compares several Blockchain architectures in terms of their impact on the integration with AI. The paper also suggests applying a use case scenario and testing the performance on several platforms in future work.

**Result**

The paper does not present any specific results as it is a conceptual paper that discusses the main factors that affect the integration of Artificial Intelligence with Blockchain. It compares several Blockchain architectures in terms of their impact on the integration with AI and suggests applying a use case scenario and testing the performance on several platforms in future work.

**Conclusion**

The paper concludes that the integration of Artificial Intelligence with Blockchain has the potential to create a self-regulated chain that can automate and forecast various processes. However, there are several factors that need to be considered, such as the cost of smart contracts, transaction fees, and storage on-chain or off-chain. The paper also highlights the need for standardization in Blockchain architecture and suggests applying a use case scenario and testing the performance on several platforms in future work.

**Future work**

The paper suggests applying a use case scenario and testing the performance on several platforms (NEO, Ethereum, Straits) to compare the latency, ease of development, and any restriction in the network. It also highlights the need for standardization in Blockchain architecture. Therefore, future work could focus on developing a standardized Blockchain architecture that can integrate with Artificial Intelligence more efficiently.

**Towards an Enterprise-Ready Implementation of Artificial Intelligence-Enabled, Blockchain-Based Smart Contracts**

**Abstract**

The paper discusses the potential of combining blockchain technology and artificial intelligence (AI) to enable smarter decision-making through AI-enabled smart contracts. It presents a new enterprise-class implementation of AI-enabled smart contracts using established standards such as Java EE, Groovy scripting language, and standardized PFA representation of ML models.

**Method**

The paper presents an approach for an enterprise-class implementation of AI-enabled smart contracts using established standards such as Java EE, Groovy scripting language, and standardized PFA representation of ML models. The approach uses the Apache Spark framework and its machine learning library to train the models, and the Portable Format for Analytics (PFA) standard to represent the trained models. The feasibility of the approach is discussed in the paper.

**Result**

The paper presents a new approach for an enterprise-class implementation of AI-enabled smart contracts using established standards such as Java EE, Groovy scripting language, and standardized PFA representation of ML models. The feasibility of the approach is discussed in the paper, but no specific results or experiments are presented. Therefore, the paper does not provide any quantitative or qualitative results.

**Conclusion**

The paper presents a new approach for an enterprise-class implementation of AI-enabled smart contracts using established standards such as Java EE, Groovy scripting language, and standardized PFA representation of ML models. The feasibility of the approach is discussed in the paper, and it is concluded that the approach is promising and can be used for real-world applications. The paper also highlights the potential benefits of combining blockchain technology and AI for smarter decision-making.

**Future work**

The paper suggests several future works that can be done to further improve the proposed approach of AI-enabled smart contracts. These include:

* Exploring the use of other machine learning model representations besides PFA.
* Investigating the use of other blockchain platforms besides Ethereum.
* Conducting experiments to evaluate the performance and scalability of the proposed approach.
* Developing tools and frameworks to simplify the development and deployment of AI-enabled smart contracts.
* Applying the proposed approach to real-world use cases in various industries, such as finance, healthcare, and supply chain management.

These future works can help to advance the field of AI-enabled smart contracts and enable their adoption in various domains.

**Overall Conclusion**

The intersection of artificial intelligence (AI) and blockchain-based smart contracts is an emerging and promising field, but one that also faces considerable challenges. Several studies have proposed novel techniques and frameworks for utilizing AI, including large language models like ChatGPT and word segmentation algorithms, to automate parts of the smart contract generation process. This demonstrates the potential for AI to replicate human drafting and greatly reduce manual effort in creating smart contracts.

However, the research also reveals risks and deficiencies in solely relying on current AI to automatically generate robust, secure smart contracts. Studies evaluating code produced by language models expose limitations in accuracy, security, and correctness - introducing bugs and vulnerabilities if deployed unchanged. Furthermore, none of the papers provide complete, step-by-step guidelines for end-to-end smart contract generation using AI.

Significant research gaps remain around prompt engineering, model training, standardized benchmarks, security enhancements, and real-world testing of AI-based smart contract generators. To mature these generative AI approaches, further work must improve model comprehension of security best practices, ensemble diverse techniques, establish rigorous evaluative frameworks, and validate performance through extensive assessments.

In conclusion, automatically generating smart contracts through AI holds immense promise to accelerate and optimize development, but remains an emerging capability. Realizing the full potential requires methodical, multi-disciplinary research to address present limitations in reliability, security, and generalization. While AI techniques can already augment and assist human creators, achieving fully autonomous generation of high-quality, robust smart contracts is still a vision requiring ongoing innovations in AI, blockchain, security, and software engineering.