University of Malta

Master of Science in Blockchain and Distributed Ledger Technologies

DLT5403: DLT and the Internet of Things

Assignment Part 1

Date Submitted: 15th September 2023
Group: Karsten Guenther
Lecturer: Prof. Joshua Ellul.

Ensuring the automation, verification, and tamper-proof nature of real-world processes is a vital aspect of modern businesses and industries. With advancements in technology and the increasing need for efficiency, transparency, and trust, organisations are seeking ways to streamline operations, validate data accuracy, and protect against unauthorised manipulation. We will explore the importance of automating, verifying, and ensuring tamper-proof processes in various domains, and delve into examples that illustrate these requirements.

One domain where automation, verification, and tamper-proofing are of utmost importance is supply chain management. The global nature of supply chains introduces complexities and risks, such as counterfeiting, theft, and unauthorised alterations. By automating supply chain processes and utilising emerging technologies like blockchain, organisations can enhance transparency and integrity throughout the supply chain. Every transaction and movement of goods can be recorded on an immutable ledger, making it possible to verify the authenticity and provenance of products. This automation and verification process not only combats counterfeiting but also ensures that goods are delivered without any tampering or unauthorised changes.

Financial transactions constitute another critical area where automation, verification, and tamper-proof measures are essential. With the rise of online banking, electronic payments, and stock trading, ensuring the integrity of financial processes has become paramount. Implementing secure authentication mechanisms, robust encryption protocols, and digital signatures can safeguard financial transactions from unauthorised access and tampering. These measures provide confidence to individuals and businesses that their financial data and transactions remain secure, accurate, and tamper-proof.

The pharmaceutical industry also relies heavily on automation, verification, and tamper-proofing to guarantee the safety and authenticity of medications. Counterfeit drugs pose a significant risk to public health, and ensuring the integrity of the pharmaceutical supply chain is crucial. By automating and verifying the entire supply chain using technologies like blockchain, it becomes possible to track the movement of drugs from manufacturing to delivery. This enables the identification of counterfeit products, ensures tamper-proof packaging, and provides assurance that medications are authentic and safe for consumption.

Food safety and traceability are paramount concerns in the food industry. Contamination, mislabelling, and unauthorised alterations can have severe health implications for consumers. Automation and verification play a vital role in enhancing food safety by tracking the origin, handling, and transportation of food products. By utilising Internet of Things (IoT) devices, sensors, and blockchain technology, organisations can monitor critical environmental factors such as temperature and humidity. This ensures the integrity of perishable goods and enables quick identification of potential issues, reducing the risk of foodborne illnesses and ensuring consumer confidence.

Automating, verifying, and ensuring the tamper-proof nature of real-world processes have become imperative in today's technologically-driven world. By embracing automation, organisations can streamline operations, improve efficiency, and minimize the risk of human error. Verification mechanisms and technologies provide confidence in the accuracy, authenticity, and integrity of data and processes. Tamper-proof measures, such as blockchain, digital signatures, and secure access controls, protect against unauthorised manipulation, ensuring the trustworthiness and reliability of real-world processes. As organisations continue to evolve and face new challenges, the demand for automation, verification, and tamper-proofing will only grow, emphasising the need for robust solutions and practices to safeguard critical operations.

IOTA is a distributed ledger technology specifically designed for the Internet of Things (IoT) ecosystem. It addresses the automation, verification, and tamper-proofing of real-world processes by providing a secure and scalable platform for machine-to-machine (M2M) transactions and data exchange.

Automation: IOTA enables automation by facilitating secure and feeless transactions between IoT devices. Through its unique Tangle architecture, IOTA eliminates the need for centralized intermediaries, allowing devices to transact and communicate autonomously. This decentralised approach promotes efficiency, reduces costs, and enables seamless automation in various IoT applications, including supply chain management, smart cities, and energy grids.

Verification and Tamper-Proofing: IOTA ensures verification and tamper-proofing by leveraging its distributed ledger technology. Transactions recorded on the Tangle are immutable and cannot be altered, providing a transparent and auditable record of events. This feature is particularly valuable in scenarios where the integrity of data or processes is crucial, such as supply chain tracking, where each transaction and movement of goods can be verified, ensuring transparency and preventing tampering.

Implementation: IOTA can be implemented through its suite of tools, including the IOTA protocol, wallets, and development frameworks. Organisations can integrate IOTA into their existing systems to enable secure and automated IoT transactions. For example, in supply chain management, IOTA's distributed ledger can be used to record and verify the movement of goods, ensuring transparency, authenticity, and tamper-proofing throughout the supply chain.

- *Supply Chain Management:* IOTA's Tangle technology can be utilized to automate and verify supply chain processes. For example, by integrating IOTA into a supply chain management system, each product can be assigned a unique digital identity recorded on the Tangle. This enables automated and tamper-proof tracking of the product's journey from manufacturing to delivery, ensuring transparency, authenticity, and reducing the risk of counterfeiting or unauthorised alterations.

- *Smart Energy Grids:* IOTA's automation capabilities can be applied to energy grids, enabling machine-to-machine transactions and peer-to-peer energy trading. Through IOTA's Tangle, IoT devices, such as solar panels and electric vehicles, can autonomously trade energy with each other based on supply and demand. This automation facilitates efficient energy distribution and reduces the need for intermediaries, ensuring tamper-proof transactions and optimizing energy usage.

ChainLink is a decentralised oracle network that connects blockchain smart contracts with real-world data and external APIs. It addresses automation, verification, and tamper-proofing by providing reliable and secure data inputs to blockchain-based processes.

Automation: ChainLink enables automation by bridging the gap between blockchain smart contracts and external data sources. Smart contracts can leverage ChainLink's decentralised oracle network to interact with off-chain data, APIs, and external systems. This automation allows for the execution of conditional actions and the integration of real-world data into blockchain processes, enhancing efficiency and enabling autonomous operations.

Verification and Tamper-Proofing: ChainLink focuses on verification and tamper-proofing by ensuring the integrity of data inputs. ChainLink oracles fetch data from multiple sources and provide it to smart contracts, creating a decentralised and tamper-resistant data feed. By aggregating data from different sources and leveraging cryptographic techniques, ChainLink ensures the accuracy and reliability of external data, reducing the risk of manipulation or unauthorised changes.

Implementation: ChainLink's decentralised oracle network can be implemented by integrating ChainLink oracles into smart contracts on various blockchain platforms. Developers can utilize ChainLink's extensive set of APIs and data sources to securely access and verify real-world data within their applications. This implementation allows for automation, verification, and tamper-proofing in various use cases, such as decentralised finance (DeFi), insurance, and supply chain management, where external data plays a crucial role.

- *Decentralised Finance (DeFi):* ChainLink plays a crucial role in DeFi applications by providing reliable and tamper-proof data feeds. For instance, in decentralised lending platforms, ChainLink oracles fetch real-time market data, such as asset prices or interest rates, from multiple sources and supply them to smart contracts. This automation ensures accurate and verifiable data for loan calculations, minimizing the risk of manipulation or unauthorised changes.
- *Insurance:* ChainLink's oracles can be used in insurance applications to automate claims verification and payout processes. For instance, in parametric insurance, where payouts are triggered based on predefined events (such as weather conditions or seismic activity), ChainLink oracles can provide real-time and tamper-proof data feeds that automatically trigger the payout process when the specified conditions are met. This automation streamlines the claims process and reduces the need for manual verification.

In the following section I will be exploring what academic research was conducted on the automation, verification, and tamper-proof nature of real-world processes. With some of the suggested research being inaccessible, other and additional research was considered for the exploration of different facets of smart contract defined IoT-behaviour, the current challenges and solutions and transitive trust.

Academic work on smart contract defined IoT-behaviour:

Smart contract-defined IoT behaviour for automatable, verifiable, and tamper-proof real-world processes is an emerging area of academic research and development. The integration of smart contracts and IoT devices has the potential to revolutionize various industries by providing secure, transparent, and efficient automation of processes. Below are presented general concepts and research directions in this field.

Automation and Interoperability: Researchers are exploring how smart contracts can enable automated interactions between IoT devices. They investigate methods to define and enforce rules for device interactions, data sharing, and decision-making in various IoT ecosystems. [1][2]

Verifiability and Consensus Mechanisms: Ensuring the verifiability of IoT behaviour is crucial for establishing trust in automated processes. Academics are studying different consensus mechanisms, such as blockchain, to enable decentralised verification and consensus for IoT-generated data and actions.[3] [4][5]

Security and Privacy: As IoT devices collect and transmit sensitive data, securing these devices and their interactions is of utmost importance. Academic work focuses on developing secure protocols, encryption methods, and access control mechanisms to protect the integrity and privacy of IoT data within smart contracts. [6] [7]

Formal Verification and Testing: Researchers are exploring formal methods to verify the correctness and safety of smart contracts that define IoT behaviour. Techniques such as model checking and formal verification help identify potential vulnerabilities or undesirable Iot-behaviour in smart contracts before deployment.[8] [9] [10]

Scalability and Performance: Since IoT ecosystems involve a large number of interconnected devices, scalability is a significant concern. Academics are investigating techniques to optimize the performance and scalability of smart contracts, considering factors such as transaction throughput, latency, and resource consumption.[11] [12]

Energy Efficiency: IoT devices are often resource-constrained, relying on limited power sources. Academic research focuses on developing energy-efficient algorithms and mechanisms to reduce the computational and communication overhead associated with executing smart contracts on IoT devices. [13][14] [15]

Legal and Regulatory Aspects: Integrating smart contracts into real-world processes raises legal and regulatory considerations. Academic work explores the legal frameworks, contract enforceability, liability, and governance models surrounding the use of smart contracts in IoT environments. [16] [17]

Academic work on current challenges and solutions:

Academic research on the challenges and solutions related to automatable, verifiable, and tamper-proof real-world processes using smart contracts and related technologies is a dynamic and evolving field. Here are a few key areas of focus on some general challenges and potential solutions that researchers have been addressing.

Scalability: One of the significant challenges is the scalability of smart contracts, particularly when applied to large-scale IoT ecosystems. Academic work explores techniques such as sharding, sidechains, and off-chain computation to improve scalability and throughput without compromising security and verifiability. [18] [19] [20]

Privacy and Data Confidentiality: Protecting the privacy and confidentiality of IoT-generated data within smart contracts is a critical concern. Researchers investigate privacy-preserving mechanisms, zero-knowledge proofs, secure multi-party computation, and homomorphic encryption to enable data privacy while ensuring verifiability and tamper-proof behaviour. [21] [22] [23]

Interoperability and Standardization: Achieving seamless interoperability between different IoT devices, platforms, and smart contract frameworks is essential for widespread adoption. Academic work focuses on developing interoperability standards, communication protocols, and middleware solutions that enable different devices and platforms to interact and execute smart contracts. [24] [25] [26]

Security and Trust: Ensuring the security and trustworthiness of smart contract-defined processes is paramount. Researchers explore techniques such as formal verification, secure coding practices, auditing tools, and bug bounty programs to identify and mitigate vulnerabilities, ensuring that smart contracts execute as intended and are resistant to tampering or unauthorised access. [27] [28] [29]

Legal and Regulatory Compliance: Integrating smart contracts into real-world processes requires consideration of legal and regulatory frameworks. Academic work investigates the legal implications of smart contracts, including issues of enforceability, liability, and jurisdiction, to ensure compliance with existing laws and explore potential regulatory frameworks for emerging use cases. [30] [31]

6. *Energy Efficiency and Resource Constraints:* IoT devices often operate with limited computational resources and energy supply. Academic research focuses on optimizing smart contracts and associated protocols to minimize resource consumption, reduce energy requirements, and improve the overall efficiency of IoT-based automated processes. [32] [33]

Academic work transitive trust:

Transitive trust is a concept that has been explored in academic research as a potential solution to address some of the challenges related to automatable, verifiable, and tamper-proof real-world processes. Transitive trust refers to the ability to establish trust relationships between entities or participants in a system based on the trustworthiness of intermediaries or third parties. Here are some ways in which transitive trust has been investigated as a solution in academic work:

Trust Hierarchies and Reputation Systems: Researchers have explored the use of trust hierarchies and reputation systems to establish transitive trust. By assigning trust values to intermediaries based on their past behaviour and reliability, these systems enable participants to trust the intermediaries and extend that trust to other entities connected through the intermediaries. [34] [35] [36]

Trust Aggregation and Consensus Mechanisms: Academic work has focused on developing trust aggregation mechanisms to combine trust ratings from multiple sources or intermediaries. Consensus mechanisms, such as blockchain-based protocols, can be used to establish trust consensus and verify the authenticity of trust ratings, ensuring the integrity and transparency of transitive trust relationships. [37] [38] [39]

Federated Learning and Secure Multiparty Computation: Transitive trust can also be established through techniques such as federated learning and secure multiparty computation. These approaches enable collaborative data analysis and decision-making while preserving privacy and maintaining trust among the participating entities. [40] [41] [42]

Semantic Trust and Contextual Information: Academic research has explored the use of semantic trust models that take into account contextual information and domain-specific knowledge. By incorporating semantic understanding of data and processes, these models enhance the accuracy and reliability of transitive trust relationships. [43] [44] [45]

Game Theory and Incentive Mechanisms: Researchers have applied game theory and incentive mechanisms to incentivise participants to act in a trustworthy manner. By aligning participants' incentives with the desired behaviour, these mechanisms promote transitive trust and discourage malicious or untrustworthy actions. [46] [47] [48]

Formal Verification of Trust Relationships: Formal verification techniques have been employed to verify the trust relationships established through transitive trust mechanisms. Formal verification techniques involve mathematically proving the correctness and security of trust relationships. This ensures that transitive trust is consistent, free from logical contradictions, and fulfils the desired properties for the specific use case. [49] [50] [51]

The convergence of blockchain, smart contracts, and IoT has opened up new possibilities for automation and trust in various industries. However, achieving a fully automated, verifiable, and tamper-proof ecosystem remains a complex and evolving challenge. In the realm of smart contracts and IoT, we have seen successful deployments in areas like supply chain management, logistics, and financial services. These applications have demonstrated the potential for automation, real-time verification, and tamper-proof record-keeping. However, scalability issues, regulatory hurdles, and interoperability challenges have hindered the widespread adoption of these technologies.

Real-world complexities, evolving threats, and the need for regulatory compliance pose ongoing challenges. Striking a balance between security and usability, ensuring energy efficiency, and addressing legal implications will require ongoing research and collaboration across multiple disciplines. Transitive trust can play a significant role in enhancing the trustworthiness and verifiability of real-world processes in IoT environments. By leveraging trust relationships established through intermediaries or third parties, transitive trust can extend trust to entities not directly known to each other. This can be particularly valuable in large-scale IoT ecosystems with diverse participants.

Transitive trust mechanisms, when combined with smart contracts, can facilitate automated decision-making based on trusted inputs from multiple sources. It can help establish more robust, reliable, and tamper-proof interactions between IoT devices and systems. Additionally, transitive trust can aid in identity management, data provenance, and access control, bolstering the overall security and verifiability of real-world processes.

However, transitive trust also introduces its own challenges, such as reliance on trusted intermediaries and the need to ensure the integrity of trust ratings. Ongoing academic research and technological advancements will be crucial in refining transitive trust mechanisms and harnessing their potential to create more secure and automated IoT-based processes.

The path to achieving fully automate-able, verifiable, and tamper-proof real-world processes is a continuous journey. As technology advances, we can expect to come closer to this ideal, but achieving absolute perfection may remain elusive due to inherent limitations and human factors. Advancements in blockchain technology, cryptographic techniques, and consensus algorithms will continue to enhance security and verifiability. Research on formal verification and auditing tools will help identify and rectify vulnerabilities in smart contracts. Standardisation efforts and interoperability protocols will facilitate seamless communication between different IoT devices and platforms.

Works Cited

[1] S. S. A. e. al., "IOT Enabled Smart Logistics Using Smart Contracts," *8th International Conference on Logistics, Informatics and Service Sciences (LISS), Toronto, ON, Canada,* no. doi: 10.1109/LISS.2018.8593220., pp. pp. 1-6, 2018.

[2] V. Jaiman and V. Urovi, "A Consent Model for Blockchain-Based Health Data Sharing Platforms," *IEEE Access ,* vol. vol. 8, no. doi: 10.1109/ACCESS.2020.3014565, pp. pp. 143734-143745, 2020.

[3] M. S. H. a. M. N. A. A. Sadawi, "A Survey on the Integration of Blockchain With IoT to Enhance Performance and Eliminate Challenges," *IEEE Access,* vol. vol. 9, no. doi: 10.1109/ACCESS.2021.3070555, pp. pp. 54478-54497,, 2021.

[4] L. C. Z. G. X. F. T. S. a. W. S. L. Xu, "DIoTA: Decentralised-Ledger-Based Framework for Data Authenticity Protection in IoT Systems," *IEEE Network,* Vols. vol. 34, no. 1, no. doi: 10.1109/MNET.001.1900136, pp. pp. 38-46, January/February 2020.

[5] B. B. M. A. A. Shivam Saxena, "Blockchain based solutions to secure IoT: Background, integration trends and a way forward," *Journal of Network and Computer Applications,* vol. Volume 181, no. https://doi.org/10.1016/, p. , 2021.

[6] Z. T. C. D. Q. Z. S. S. a. B. F. J. Qiu, "A Survey on Access Control in the Age of Internet of Things," *IEEE Internet of Things Journal,* Vols. vol. 7, no. 6, no. doi: 10.1109/JIOT.2020.2969326, pp. pp. 4682-4696, June 2020.

[7] E. F. A. K. A. A. A. E. A. K. Y. M. Algarni S, "Blockchain-Based Secured Access Control in an IoT System," *Applied Sciences,* no. https://doi.org/10.3390/app11041772, p. 11(4):1772. , 2021.

[8] K. K. W. G. a. M. G. Ikram Garfatta, "A Survey on Formal Verification for Solidity Smart Contracts," in *Proceedings of the 2021 Australasian Computer Science Week Multiconference (ACSW '21). Association for Computing Machin*, 2021.

[9] L. S. A. E. S. A. M. Mouhamad Almakhour, "Verification of smart contracts: A survey," *Pervasive and Mobile Computing,* vol. Volume 67, no. https://doi.org/10.1016/j.pmcj.2020.101227, 2020.

[10] R. M. P. Q. Z. Amritraj Singh, "Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities," *Computers & Security,* vol. Volume 88, no. https://doi.org/10.1016/j.cose.2019.101654, 2020.

[11] M. E. Y. a. M. L. A. Nag, "Blockchain for 5G and IoT: Opportunities and Challenges doi: 10.1109/ComNet47917.2020.93060," in *IEEE Eighth International Conference on Communications and Networking (ComNet),* , Hammamet, Tunisia., 2020.

[12] K. P. R. E. Sudeep Tanwar, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications," *Journal of Information Security and Applications,* vol. Volume 50, no. https://doi.org/10.1016/j.jisa, p. 2020.

[13] A. A. U. A. N. K. M. K. H. Ullah I, "An Energy Efficient and Formally Secured Certificate-Based Signcryption for Wireless Body Area Networks with the Internet of Things.," *Electronics. ,* no. https://doi.org/10.3390/electronics81, 2019; .

[14] K. J. D. a. P. P. D. S. Alex, "Private and Energy-Efficient Decision Tree-Based Disease Detection for Resource-Constrained Medical Users in Mobile Healthcare Network," *IEEE Access,* vol. vol. 10, no. doi: 10.1109/ACCESS.202, pp. pp. 17098-17112, 2022.

[15] M. H. D. P. a. H. S. T. Ma, "A Survey of Energy-Efficient Compression and Communication Techniques for Multimedia in Resource Constrained Systems,," *IEEE Communications Surveys & Tutorials,* Vols. vol. 15, no. 3, no. doi: 10.1109/SURV.2012.060912.00149, pp. pp. 963-972,, Third Quarter 2013.

[16] Agata Ferreira, "Regulating smart contracts: Legal revolution or simply evolution?," *Telecommunications Policy,* Vols. Volume 45, Issue 2, no. https://doi.org/10.1016/j.telpol.2020.102081, 2021 .

[17] J. E. a. J. -H. Morin, "Towards Governance and Dispute Resolution for DLT and Smart Contracts doi: 10.1109/ICSESS.2018," in *IEEE 9th International Conference on Software Engineering and Service Science (ICSESS)*, Beijing, China, 2018 .

[18] H. H. Z. Z. a. J. B. Q. Zhou, "Solutions to Scalability of Blockchain: A Survey," *IEEE Access,* vol. Vol. 8, no. Doi: 10.1109/ACCESS.2020.2967218, pp. pp. 16440-16455, 2020.

[19] M. A. a. O. L. C. Profentzas, ""TinyEVM: Off-Chain Smart Contracts on Low-Power IoT Devices,"," in *IEEE 40th International Conference on Distributed Computing Systems (ICDCS),* , Singapore, 2020.

[20] C. L. H. X. a. S. P. Di Yang, " A Review on Scalability of Blockchain. In Proceedings of the 2020 The 2nd International Conference on Blockchain Technology (ICBCT'20)," in *Association for Computing Machinery,* , New York, NY, USA, 2020..

[21] S. R. D. Sawant, "Privacy Preserving Algorithm for Blockchain-Based IOT System.," in *Information and Communication Technology for Competitive Strategies (ICTCS 2022).* , (2023).

[22] S. A. Wright, "Privacy in IoT Blockchains: with Big Data comes Big Responsi-bility,," in *IEEE International Conference on Big Data (Big Data),* , Los Ange-les, CA, USA, 2019, pp. 5282-5291, doi: 10.1109/BigData47090.2019.9006341., 2019 .

[23] F. Y. W. Z. G. D. Zhou J, "Using Secure Multi-Party Computation to Protect Privacy on a Permissioned Blockchain," in *Sensors*, 2021 https://doi.org/10.3390/s21041540.

[24] R. P. C. M. M. L. A. F. Gravina, "Towards Multi-layer Interoperability of Heterogeneous IoT Platforms: The INTER-IoT Approach.," *Integration, Interconnection, and Interoperability of IoT Systems. Internet of Things.,* 2018.

[25] A. A. A. S. N. A. M. Y. A. A. a. N. M. B. S. S. Albouq, "A Survey of Interoperability Challenges and Solutions for Dealing With Them in IoT Environment," *IEEE Access,* vol. vol. 10, no. doi: 10.1109/ACCESS.202, pp. pp. 36416-36428, 2022.

[26] H. H. M. Rahman, " A comprehensive survey on semantic interoperability for Internet of Things: State-of-the-art and research challenges.," *Trans Emerging Tel Tech,* vol. 31:e3902. , no. https://doi.org/10.1002/ett.3902, 2020.

[27] Y. H. J. Z. N. e. a. Wang, "Security enhancement technologies for smart contracts in the blockchain: A survey.," *Trans Emerging Tel Tech. ,* vol. 32(12) , no. https://doi.org/10.1002/ett.4341, 2021; .

[28] W. Zou et al., "Smart Contract Development: Challenges and Opportunities," *IEEE Transactions on Software Engineering,* Vols. vol. 47, no. 10, no. Doi: 10.1109/TSE.2019.2942301., pp. pp. 2084-2106, 2021.

[29] S. R. a. R. Deters, "Security, Performance, and Applications of Smart Contracts: A Systematic Survey," *IEEE Access,* vol. vol. 7, no. Doi: 10.1109/ACCESS.2019.2911031, pp. pp. 50759-50779, 2019.

[30] J. Madir, "mart Contracts: (How) Do They Fit Under Existing Legal Frameworks?," no. http://dx.doi.org/10.2139/ssrn.3301463, 2018.

[31] Agata Ferreira, "Regulating smart contracts: Legal revolution or simply evolution?,," *Telecommunications Policy, ,* Vols. Volume 45, Issue 2, , no. https://doi.org/10.1016/j.telpol.2020.102081., 2021,.

[32] ". J. Ellul and G. J. Pace, "AlkylVM: A Virtual Machine for Smart Contract Blockchain Connected Internet of Things,"," in *9th IFIP International Conference on New Technologies,*, Paris France, 2018 .

[33] A. A. W. A. A. L. A. R. G. I. A. A. a. B. A. T. A. Ayub Khan, "BIoMT: A State-of-the-Art Consortium Serverless Network Architecture for Healthcare System Using Blockchain Smart Contracts," *IEEE Access,* vol. vol. 10, no. pp. 78887-78898.

[34] X. Liu and L. Xiao, ""hiREP: Hierarchical Reputation Management for Peer-to-Peer Systems,," in *Doi: 10.1109/ICPP.2006.48.*, Columbus, OH, USA, , 2006 International Conference on Parallel Processing (ICPP'06), .

[35] I. -R. C. M. C. a. J. -H. C. F. Bao, "Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection,"," *IEEE Transactions on Network and Service Management, ,* Vols. vol. 9, no. 2, pp. 1.

[36] F. G.-G. G. G.-S. M. E. H. a. M. L. I. Martínez-Sarriegui, "TRHIOS: Trust and reputation in hierarchical and quality-oriented societies," in *7th Iberian Conference on Information Systems and Technologies*, Madrid, Spain, 2012.

[37] S. B. S. S. H. L. I. K. M. A. Sowmya Kudva, "A scalable blockchain based trust management in VANET routing protocol," *Journal of Parallel and Distributed Computing,* vol. Volume 152, no. https://doi.org/10.1016/j.jpdc.2021.02.024., pp. Pages 144-156, 2021.

[38] K. Y. L. L. K. Z. a. V. C. M. L. Z. Yang, "Blockchain-Based Decentralised Trust Management in Vehicular Networks," *IEEE Internet of Things Journa,* Vols. vol. 6, no. 2, no. Doi: 10.1109/JIOT.2018.2836144, pp. pp. 1495-1505, April 2019.

[39] F. C. E. H.-V. Jian Wu, "Trust based consensus model for social network in an incomplete linguistic information context," *Applied Soft Computing,* vol. Volume 35, no. https://doi.org/10.1016/j.asoc.2015, pp. Pages 827-839, 2015.

[40] Y. Z. A. J. D. Y. G. X. a. X. Z. Y. Li, "Privacy-Preserving Federated Learning Framework Based on Chained Secure Multiparty Computing," *IEEE Internet of Things Journal,* Vols. vol. 8, no. 8, no. Doi: 10.1109/JIOT, pp. pp. 6178-6186, 2021.

[41] N. B. A. A. T. S. H. L. R. Z. a. Y. Z. 2. Stacey Truex, "A Hybrid Approach to Privacy-Preserving Federated Learning.," in *In Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security (AISec'19)*, NY,USA, 2019.

[42] A. K. S. A. T. a. V. S. T. Li, "Federated Learning: Challenges, Methods, and Future Directions,," *IEEE Signal Processing Magazine,* Vols. vol. 37, no. 3, no. Doi: 10.1109/MSP.2020.2975749, pp. pp. 50-60, , May 2020, .

[43] N. a. M. M. Dokoohaki, "Effective design of trust ontologies for improvement in the structure of socio-semantic trust networks.," *International Journal On Advances in Intelligent Systems ,* 2008.

[44] K. A. a. Z. Despotovic., "Managing trust in a peer-2-peer information system," in *Proceedings of the tenth international conference on Information and knowledge management (CIKM '01). Association for Computing Machinery*, New York, NY, USA,, 2001.

[45] R. M. a. Y. D. F. Ramparany, "A Semantic Approach for Managing Trust and Uncertainty in Distributed Systems Environments," in *21st InternationaConference on Engineering of Complex Computer Systems (ICECCS)*, Dubai, United Arab Emirates, 2016.

[46] C. Z. X. W. B. L. a. X. C. R. Zeng, "Incentive Mechanisms in Federated Learning and A Game-Theoretical Approach," *IEEE Network,* Vols. Vol. 36, no. 6, no. Doi: 10.1109/MNET.112.2100706., pp. pp. 229-235, 2022.

[47] W.-T. L. N. G. T.-M. W. Tin-Yu Wu, "Incentive mechanism for P2P file sharing based on social network and game theory," *Journal of Network and Computer Applications,* vol. Volume 41, no. https://doi.org/10.101, pp. Pages 47-55, 2014.

[48] Q. L. S. W. Z. C. Q. B. Xiang Li, "Game theory based compatible incentive mechanism design for non-cryptocurrency blockchain systems,," *Journal of Industrial Information Integration,,* Vols. Volume 31,, no. https://doi.org/10.1016/j.jii.2022.100426., 2023.

[49] A. Jøsang, "The right type of trust for distributed systems.," in *Proceedings of the 1996 workshop on New security paradigms*, 1996 .

[50] N. B. J. L. A. e. a. Drawel, "Formal verification of group and propagated trust in multi-agent systems.," *Auton Agent Multi-Agent,* no. https://doi.org/10.1007/s10458-021-09542-6, 2022.

[51] B. S. Katharina Hofer-Schmitz, " Towards formal verification of IoT protocols: A Review," *Computer Networks,* vol. Volume 174, no. https://doi.org/10.1016/j.comnet.2020.107233, 2020.