ST.GALLEN SYMPOSIUM

Global Essay Competition 2025

Title: Decentralized Proof-of-Location as a Future Pillar of Digital Sovereignty, Trust, and Security in a Multipolar Era

Essay:

The world is undergoing a profound transformation as emerging economies across Asia, Africa, and Latin America assert themselves as new centres of technological, economic, and geopolitical power. This shift is not merely a redistribution of economic influence but a fundamental restructuring of the digital landscape. As societies undergo rapid digitalization, their ability to sustain independent technological ecosystems is becoming a defining factor in their long-term internal stability, external competitiveness, and global cooperation. The ability to develop and govern its own critical digital infrastructure, without reliance on external actors, is now central to national sovereignty, emerging as a key pillar of modern statecraft.

The dynamics of digital trust as a geopolitical game

At the heart of this transformation is the evolution of trust in digital societies. Trust, once embedded in traditional national or international institutions such as governments, financial intermediaries, and legal frameworks, is increasingly being shaped by technological innovations and the infrastructures that enable secure digital interactions. The foundation of modern economies, governance, and even social cohesion now relies on the ability to verify identities, transactions, and information in a digital-first world [39, 43]. The rise of e-government platforms, digital financial systems, smart cities, and AI-driven decision-making has placed immense pressure on each nation to ensure that the digital infrastructures underpinning these services are both reliable and sovereign [31]. In this context, the concept of technological resilience is taking centre stage, as countries recognize the risks of relying on foreign-controlled verification systems, cloud services, and digital identity frameworks [7, 32, 37].

Nonetheless, the integrity of digital trust mechanisms extends beyond national boundaries and is also an important means for international cooperation, reputation, and accountability [37]. It is set to shape the stability of global supply chains, the enforceability of international law, and the security of cross-border transactions [28]. In an era of deeply interconnected economies, businesses will increasingly depend on verifiable data to ensure the authenticity and tamper-resistance of trade agreements, the traceability of goods, and the security of international investments [2]. Similarly, global institutions and legal frameworks will have to rely on trusted digital verification systems to uphold international contracts, enforce regulations, and mitigate cross-border cybercrime [16]. The ability of a nation to maintain secure and sovereign digital infrastructures not only will determine its internal resilience but also its credibility and reliability as a global actor. Without secure, independent verification mechanisms, nations risk being sidelined in economic, democratic, and diplomatic engagements, as trust in their partnerships becomes increasingly uncertain. Concurrently to this, the rapid and decentralized

digitalization of nations also signifies the emergence of new threat landscapes in geopolitical warfare, with states and non-state actors alike developing increasingly sophisticated capabilities to manipulate, disrupt, and destabilize adversaries for strategic advantage [7, 25, 36]. The very infrastructures that facilitate digital sovereignty may become key battlegrounds where cyberattacks, misinformation campaigns, and systemic fraud are deployed to undermine trust at both national and global levels.

Therefore, digital interactions growing more integral to governance, economic stability, and international cooperation means that the capacity to both ensure verifiable, tamper-proof digital trust and to defend against these adversarial strategies will define not only a nation's internal security, but also its influence and legitimacy in the international order.

Emerging digital societies lack location proving infrastructures

In fact, the contest over digital sovereignty has already made trust infrastructure manipulation a core tactic of cyberwarfare, as adversaries exploit verification system weaknesses to distort public perception, disrupt governance, and destabilize economies. One of the most concerning developments has been the weaponization of AI-powered misinformation, using falsified identities, synthetic media, and location spoofing to undermine trust in democratic institutions and international relations [22]. The 2016 U.S. election interference, orchestrated by Russian intelligence via the Internet Research Agency, demonstrated how adversarial actors can fabricate digital identities at scale, simulating online activity to manipulate public discourse [8]. Thousands of fake social media accounts, posing as U.S. citizens, spread divisive content, staged protests, and amplified false narratives, all while spoofing geolocation data to appear domestic. Similarly, in Brazil's 2018 and 2022 elections, misinformation networks flooded WhatsApp and Telegram with AI-generated videos, fake voice recordings, and fabricated reports, eroding trust in electoral processes [9, 13, 40]. The current nature of digital platforms makes verification nearly impossible, allowing false geolocation data to simulate political protests, voting irregularities, and electoral fraud. In both cases, the failure of verification mechanisms enabled these narratives to spread uncontested, fuelling polarization and distrust.

Beyond election interference, cyberwarfare has increasingly targeted real-time location authentication in modern military conflicts, where control over digital trust mechanisms can shape both battlefield operations and global narratives. Falsified geolocation data, GPS spoofing, and synthetic satellite imagery have misled military intelligence, disrupted logistics, and distorted public perceptions of conflicts. In the Russia-Ukraine war, pro-Kremlin actors systematically deployed AI-generated images and geotagged social media posts to fabricate incidents of Ukrainian aggression, shaping early international reactions [11, 24]. Meanwhile, GPS spoofing in contested zones has interfered with drone navigation, military coordination, and civilian evacuations [19]. Similarly, in the Israel-Palestine conflict, falsified location-tagged videos and doctored battlefield images have been used to manipulate public opinion, with both state and non-state actors leveraging AI-created content to justify military actions or discredit adversaries [21].

Cybercriminal networks and state-backed actors have also exploited location fraud to infiltrate global supply chains, bypass trade regulations, counterfeit products, and commit large-scale financial fraud. The 2019 Wirecard scandal [20], one of Europe's largest financial fraud cases, revealed how fabricated location data was used to create fake business operations, generate false customer transactions, and deceive regulators about the company's financial stability. Similarly, fraudulent supply chain practices have plagued the food [33], pharmaceutical [6], and fashion industries [1], where falsely certified origins allow everything from

non-organic crops to counterfeit medicines and mislabelled luxury goods to enter global markets unchecked [29]. Hacking groups from around the world have also used location spoofing to evade sanctions, laundering stolen digital currencies through decentralized exchanges that lacked robust verification mechanisms [27].

These and many other cases highlight an urgent reality: the inability to reliably verify geolocation claims is boosting cyberwarfare, financial fraud, and mass disinformation at an unprecedented scale. Existing digital trust infrastructures, built on centralized databases and proprietary geolocation services, have proven inadequate against evolving threats [23]. The reliance on weak, static credentials and uncontrolled verification systems has allowed adversaries to manipulate location-based data with ease, distorting public perception, destabilizing economies, and eroding governance structures [3]. To counter these vulnerabilities, cryptographically verifying presence and geolocation in a tamper-resistant manner is essential to securing digital interactions [18, 34]. By leveraging distributed validation, cryptographic attestation, and consensus-based verification models, decentralized location proving systems can ensure that geolocation data is verifiable, censorship-resistant, and resilient to manipulation [17]. As global power shifts, nations that integrate location proving into their digital sovereignty strategies will be best positioned to secure both internal and global trust infrastructures in an increasingly adversarial digital landscape.

Decentralized Proof-of-Location for advancing digital sovereignty, trust, and security

Given these escalating challenges, I argue that decentralized Proof-of-Location infrastructures must become a foundational pillar in the digital transformation strategies of nations, reinforcing sovereignty, trust, and security in an era where global power dynamics are increasingly defined by digital credibility. The ability to verify location in a cryptographically secure and tamper-proof manner is no longer a niche technical concern but a geopolitical necessity. As shown, the manipulation of location data has already been exploited to undermine democratic processes, disrupt economies, and distort military intelligence. The absence of a verifiable, independent mechanism for proving physical presence has enabled adversarial actors to falsify geospatial claims, propagating disinformation, financial fraud, and cyberwarfare. In response, I propose that Proof-of-Location infrastructures should be developed to serve as a critical safeguard, empowering nations to assert digital sovereignty, fortify their role in global governance, and stabilize the societal trust upon which both domestic security and international cooperation depend.

The concept of Proof-of-Location has evolved in direct response to the growing demand for secure and tamper-resistant geolocation authentication [5, 17, 44]. Traditional location verification systems have long relied on centralized models, such as the Global Positioning System (GPS), cell tower triangulation, and Wi-Fi positioning, all of which are controlled by a handful of entities and do not work in adversarial environments [12, 44]. While these systems have enabled navigation, logistics, and digital verification across industries, they introduce critical vulnerabilities. GPS signals, for instance, are highly susceptible to spoofing and jamming, allowing attackers to falsify location data and manipulate supply chain networks, geotagged content, or military logistics. Likewise, cell tower-based verification depends on telecommunications providers, which operate under regulatory constraints, geopolitical influence, and external control [41]. These structural weaknesses underscore the urgent need for a more resilient and censorship-resistant approach. As a result, decentralized and cryptographically verifiable Proof-of-Location infrastructures have emerged as the logical evolution, reducing dependence on single points of failure while enhancing resistance to manipulation and systemic

fraud [17, 38].

At a national scale, a decentralized Proof-of-Location infrastructure would function as a physically deployed network of independent verification devices — witnesses — that collaboratively attest to location claims in a secure and tamper-resistant manner [17]. Instead of relying on a single centralized authority, such system would distribute trust across a latticework of witnesses deployed throughout a territory. These witnesses could be stationary sensors, mobile devices, or infrastructure-embedded units [15, 42], and would interact with provers — the individuals, devices, or systems seeking to verify their location. Unlike traditional location services, which are prone to spoofing and external control, this decentralized model ensures that no single entity has absolute control over location verification. When a prover requests a location proof, nearby witnesses engage in cryptographic exchanges, confirming the prover's presence through secure distance measurements and digital signatures [4]. Once a sufficient number of witnesses agree on the nearby presence of the prover, they collectively sign an attestation that is recorded on a tamper-proof ledger, making it verifiable for a myriad of use cases [17]. This infrastructure would also incorporate synchronized time-stamping to ensure that location claims are both spatially and temporally valid [26], preventing retroactive falsification. By structuring the witness network into overlapping geographic zones, such system would also allow for flexible verification levels, ranging from highly precise local confirmations to broader regional attestations.

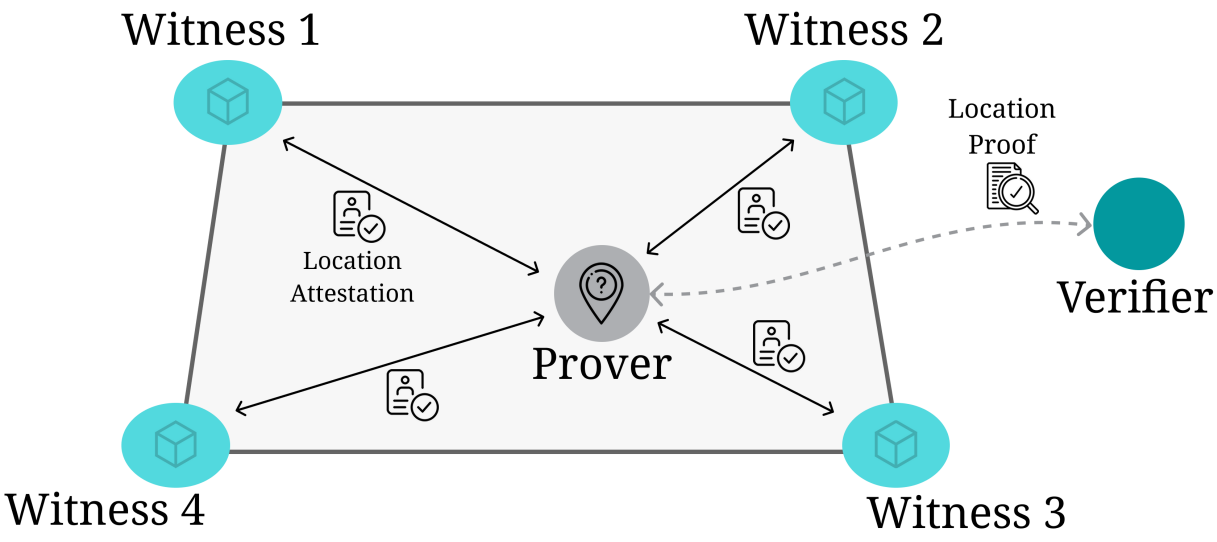

Figure 1: A location proof is a verifiable digital certificate that cryptographically attests the presence of a prover, at a particular location and time, by a set of witnesses.

A national Proof-of-Location infrastructure would establish a verifiable, tamper-resistant method for proving location, eliminating reliance on external authorities while ensuring security, scalability, and privacy. As a pillar of trust in digital societies, it would protect against adversarial threats that manipulate location-based data for economic, political, or strategic gain. By enabling independently verifiable location claims, Proof-of-Location would safeguard democratic processes from election fraud and disinformation [38, 46], reinforce economic stability by preventing financial and trade fraud, and enhance international cooperation by securing supply chains [35] and deterring illicit activities like smuggling and cybercrime. In crisis management and defence, Proof-of-Location would provide real-time situational awareness, ensuring the authenticity of humanitarian aid deliveries, disaster response coordination, and military operations. Many other applications would benefit, including verifying citizen participation in public

decision-making [38], securing subsidy programs by confirming recipients' physical presence, enhancing public transportation with cryptographic proofs of ridership [10, 30], strengthening liability frameworks through immutable location records, ensuring regulatory compliance in infrastructure deployment [45], securing delivery services with verifiable handovers [35], authenticating the physical originality of digital media [22], preventing fraud in location-based retail incentives [41], or enforcing geographic restrictions for digital content distribution [44].

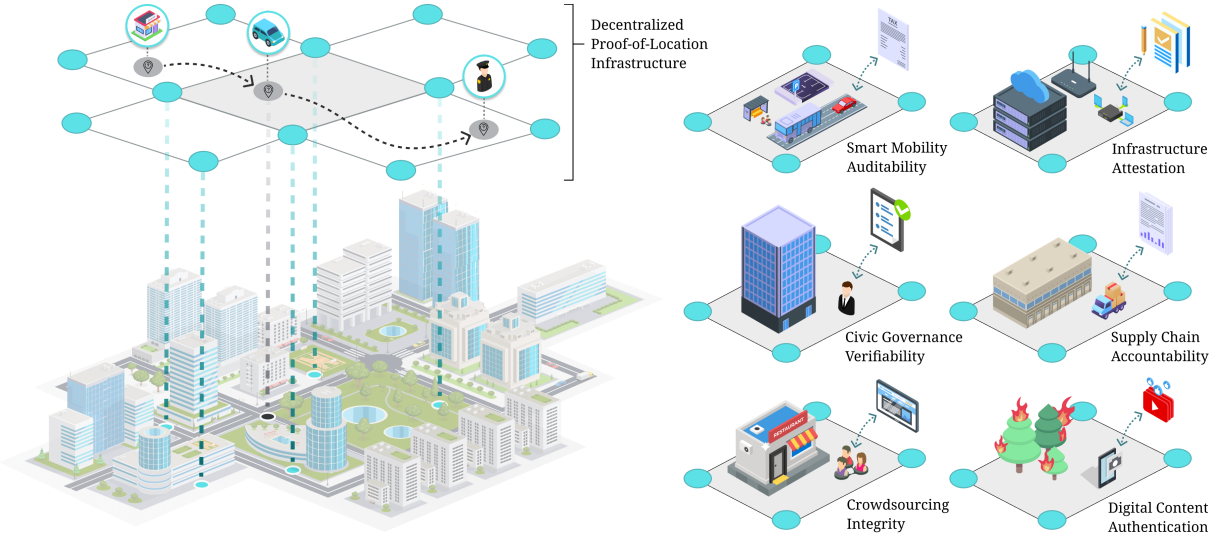

Figure 2: Application scenarios for a Decentralized Proof-of-Location infrastructure.

By establishing verifiable presence as a core digital primitive [14], Proof-of-Location would empower nations to assert greater digital sovereignty in an era where digital trust is increasingly contested. As global power shifts towards a multipolar order, the ability to independently verify location-based claims will be a defining pillar of economic resilience, governance legitimacy, and international cooperation. Nations that deploy Proof-of-Location infrastructures will not only secure their digital and territorial sovereignty but also cement their position as trusted actors in global trade, cybersecurity, and diplomacy. More broadly, Proof-of-Location would strengthen the integrity of both digital and physical interactions, enabling a more accountable, resilient, and geopolitically autonomous global landscape — one where trust is anchored in cryptographic certainty rather than unverifiable claims.

Reference List / Bibliography / Sources:

[1] Tarun Kumar Agrawal, Vijay Kumar, Rudrajeet Pal, Lichuan Wang, and Yan Chen. Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry. *Computers & industrial engineering*, 154:107130, 2021.

[2] Usman Ahmed. The importance of cross-border regulatory cooperation in an era of digital trade. *World Trade Review*, 18(S1):S99–S120, 2019.

[3] Mamunur Rashid Akand, Reihaneh Safavi-Naini, Mark Kneppers, Matthieu Giraud, and Pascal Lafourcade. Privacy-preserving proof-of-location with security against geo-tampering. *IEEE Transactions on Dependable and Secure Computing*, 2021.

[4] Md Mamunur Rashid Akand. *Contribution to Proof-of-Location Systems.* PhD thesis, University of Calgary, Alberta, Canada, 2023.

[5] Michele Amoretti, Giacomo Brambilla, Francesco Medioli, and Francesco Zanichelli. Blockchain-based proof of location. In *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, pages 146–153. IEEE, 2018.

[6] Archa, Bithin Alangot, and Krishnashree Achuthan. Trace and track: Enhanced pharma supply chain infrastructure to prevent fraud. In *Ubiquitous Communications and Network Computing: First International Conference, UBICNET 2017, Bangalore, India, August 3-5, 2017, Proceedings 1*, pages 189–195. Springer, 2018.

[7] Itzhak Aviv and Uri Ferri. Russian-ukraine armed conflict: Lessons learned on the digital ecosystem. *International Journal of Critical Infrastructure Protection*, 43:100637, 2023.

[8] Adam Badawy, Aseel Addawood, Kristina Lerman, and Emilio Ferrara. Characterizing the 2016 russian ira influence campaign. *Social Network Analysis and Mining*, 9:1–11, 2019.

[9] Frederico Batista Pereira, Natália S Bueno, Felipe Nunes, and Nara Pavão. Fake news, fact checking, and partisanship: the resilience of rumors in the 2018 brazilian elections. *The Journal of Politics*, 84(4):2188–2201, 2022.

[10] Felipe Boeira, Mikael Asplund, and Marinho Barcellos. Decentralized proof of location in vehicular ad hoc networks. *Computer Communications*, 147:98–110, 2019.

[11] Roger Canals. Visual trust: Fake images in the russia-ukraine war. *Anthropology Today*, 38(6):4–7, 2022.

[12] Srdjan Capkun and J-P Hubaux. Secure positioning in wireless networks. *IEEE Journal on Selected Areas in Communications*, 24(2):221–232, 2006.

[13] Regina Cazzamatta and Augusto Santos. Checking verifications during the 2022 brazilian run-off election: How fact-checking organizations exposed falsehoods and contributed to the accuracy of the public debate. *Journalism*, 25(10):2022–2043, 2024.

[14] Nishanth Chandran, Vipul Goyal, Ryan Moriarty, and Rafail Ostrovsky. Position based cryptography. In *Annual International Cryptology Conference*, pages 391–407. Springer, 2009.

[15] Antonio Cilfone, Luca Davoli, Laura Belli, and Gianluigi Ferrari. Wireless mesh networking: An iot-oriented perspective survey on relevant technologies. *Future Internet*, 11(4):99, 2019.

[16] Jared Cohen and Richard Fontaine. Uniting the techno-democracies: How to build digital cooperation. *Foreign Aff.*, 99:112, 2020.

[17] Foamspace Corp. Foam whitepaper. Accessed: 2025-01-28.

[18] Aurélien Dupin, Jean-Marc Robert, and Christophe Bidan. Location-proof system based on secure multi-party computations. In *Provable Security: 12th International Conference, ProvSec 2018, Jeju, South Korea, October 25-28, 2018, Proceedings*, pages 22–39. Springer, 2018.

[19] Sitki Egeli. Emerging and disruptive technologies in russia's war against ukraine. In *Russia's War on Ukraine: The Implications for the Global Nuclear Order*, pages 55–68. Springer, 2023.

[20] Klaus C Engelen. Germany's wirecard scandal. *The International Economy*, 35(1):9–12, 2021.

[21] Sheera Frenkel. Lies on social media inflame israeli-palestinian conflict. *International New York Times*, pages NA–NA, 2021.

[22] Jeffrey T Hancock and Jeremy N Bailenson. The social impact of deepfakes, 2021.

[23] Chitra Javali, Girish Revadigar, Kasper B Rasmussen, Wen Hu, and Sanjay Jha. I am alice, i was in wonderland: secure location proof generation and verification protocol. In *2016 IEEE 41st conference on local computer networks (LCN)*, pages 477–485. IEEE, 2016.

[24] Irina Khaldarova and Mervi Pantti. Fake news: The narrative battle over the ukrainian conflict. In *The Future of Journalism: Risks, Threats and Opportunities*, pages 228–238. Routledge, 2020.

[25] Aneel Waqas Khan, Sarah Saeed, and M Saleem Kakar. Cybersecurity as a geopolitical tool: The growing influence of digital warfare in statecraft. *International Research Journal of Social Sciences and Humanities*, 3(2):345–357, 2024.

[26] Ryan John King. Foam: The importance of time synchronization. *Medium*, Feb 2020. Accessed: 2025-01-28.

[27] Bruce Klingner. North korean cyberattacks: A dangerous and evolving threat. *The Heritage Foundation*, 2021.

[28] M Larionova and A Shelepov. Emerging regulation for the digital economy: Challenges and opportunities for multilateral global governance. *International Organisations Research Journal*, 16(1):29–63, 2021.

[29] Ling Li. Technology designed to combat fakes in the global supply chain. *Business Horizons*, 56(2):167–177, 2013.

[30] Wanxin Li, Collin Meese, Zijia Gary Zhong, Hao Guo, and Mark Nejad. Location-aware verification for autonomous truck platooning based on blockchain and zero-knowledge proof. In *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 1–5. IEEE, 2021.

[31] Miriam Lips. Rethinking citizen–government relationships in the age of digital identity: Insights from research. *Information Polity*, 15(4):273–289, 2010.

[32] Gulsanna Mamediieva and Donald Moynihan. Digital resilience in wartime: The case of ukraine. *Public Administration Review*, 83(6):1512–1516, 2023.

[33] Louise Manning. Food fraud: Policy and food chain. *Current Opinion in Food Science*, 10:16–21, 2016.

[34] Bulat Nasrulin, Muhammad Muzammal, and Qiang Qu. A robust spatio-temporal verification protocol for blockchain. In *Web Information Systems Engineering–WISE 2018: 19th International Conference, Dubai, United Arab Emirates, November 12-15, 2018, Proceedings, Part I 19*, pages 52–67. Springer International Publishing, 2018.

[35] Mohammad Reza Nosouhi, Shui Yu, Marthie Grobler, Yong Xiang, and Zuqing Zhu. Sparse: privacy-aware and collusion resistant location proof generation and verification. In *2018 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6. IEEE, 2018.

[36] Kieron O'hara and Wendy Hall. Four internets: The geopolitics of digital governance. 2018.

[37] Julia Pohle and Thorsten Thiel. Digital sovereignty. *Pohle, J. & Thiel*, 2020.

[38] Evangelos Pournaras. Proof of witness presence: Blockchain consensus for augmented democracy in smart cities. *Journal of Parallel and Distributed Computing*, 145:160–175, 2020.

[39] Jiří Prša. E-identity: Basic building block of e-government. In *2015 IST-Africa Conference*, pages 1–10. IEEE, 2015.

[40] Eliara Santana and Isabele Mitozo. Disinformation and democracy: The strategies for institutional dismantle in brazil (2018–2022). In *Social Policies in Times of Austerity and Populism*, pages 89–106. Routledge.

[41] Stefan Saroiu and Alec Wolman. Enabling new mobile applications with location proofs. In *Proceedings of the 10th workshop on Mobile Computing Systems and Applications*, pages 1–6, 2009.

[42] Mihail L Sichitiu. Wireless mesh networks: opportunities and challenges. In *Proceedings of World Wireless Congress*, volume 2, page 21, 2005.

[43] Jeff Stapleton and W Clay Epstein. *Security without Obscurity: A Guide to PKI Operations*. CRC Press, Boca Raton, Florida, USA, 2024.

[44] Brent Waters and Edward Felten. Secure, private proofs of location. *Department of Computer Science, Princeton University, Tech. Rep. TR-667-03*, 2003.

[45] Faheem Zafar, Abid Khan, Adeel Anjum, Carsten Maple, and Munam Ali Shah. Location proof systems for smart internet of things: Requirements, taxonomy, and comparative analysis. *Electronics*, 9(11):1776, 2020.

[46] Xinyi Zhou and Reza Zafarani. A survey of fake news: Fundamental theories, detection methods, and opportunities. *ACM Computing Surveys (CSUR)*, 53(5):1–40, 2020.

Note: In preparing this essay, various tools were used to enhance readability, accuracy, and presentation. ChatGPT assisted in refining grammar, readability, and word choice, while, together, Google, ChatGPT, and Perplexity AI were used adversarially to fact-check arguments and verify the correctness of information against cited sources. Cspell and LTeX provided spelling and grammar checks in a local LaTeX writing environment. For visuals, vectors and icons from Flaticon and Freepik were used, and Figma was employed for image creation and editing. All these tools were used solely to support clarity, correctness, and layout, maintaining the originality and integrity of my work.

Word Count (essay text only): (2036 / 2100)