Crypto-Spatial: A New Direction in Geospatial Data

Darshana Rawal [1], Salvatore Amaduzzi[2], Jan Seedorf [1]

[1] Hochschule für Technik Stuttgart, University of Applied Sciences, Schellingstr. 24, 70174 Stuttgart – (darshana.rawal, jan.seedorf)@hft-stuttgart.de

[2] University of Udine, Via Palladio, 8, 33100 Udine UD, Italy - salvatore.amaduzzi@uniud.it

Keywords: Cryptography, Geospatial Data, Block Chain, Web3.0, Geospatial Data

Abstract

Geospatial technology involves the use of maps, satellite imagery, and spatial databases to collect, analyze, and visualize geographic data. Understanding the link between blockchain and geospatial technology is crucial as it opens the door to innovation and progress in both fields. “The use of Blockchain as a system for managing and verifying geospatial data necessitates accuracy, integrity, and trustworthiness”(Pengxiang et al 2022). Improving data integrity, promoting collaboration, and revolutionizing applications in the geospatial domain are all possible through the combination of these two technologies.

The World Wide Web (WWW) has expanded connections worldwide, but it also makes networks susceptible to multiple attacks from various anonymous sources. Packets of fixed or variable sizes are used for transmitting data across nodes. Data is encrypted using secure algorithms at the application level, then packetized and sent at lower levels in the OSI architecture. The encrypted data can be obtained by an intruder by organizing the data contents of each packet once they have access to all the packets. Intruders may also attempt to break the secured algorithm used by the sender.

This sophisticated approach to Data Security is the content and order of data, ensuring that unauthorized individuals are unable to discern sensitive information during data transmission. The primary objective of this paper is to introduce a novel spatial encryption technique designed to enhance the security of data transfers within networks. This paper, founded on a comprehensive literature review, endeavors to propose a research project focused on exploring futuristic solutions, particularly within the post-quantum era.

1. Introduction

The future of the Internet is built on innovative and optimistic ideas such as decentralized computing, digital dominion, and seamless integration between the digital and non-digital worlds. This marks a shift from the Internet's current centralized approach, where data is hosted by a single entity, to a decentralized model where data is distributed among peers in a network. The evolution of internet infrastructures from Web 2.0 to Web 3.0 is largely driven by blockchain technologies. Decentralized applications (dApps) are designed without any single entity having undue control or influence over the system. This integration of new technologies creates a three-dimensional computing environment, forming a spatial web that gives users greater choice and power.

The goal of Web3 is to provide individuals with the necessary tools to communicate directly with each other, eliminating the need for intermediaries who extract value. Despite being the early pioneers of this new age, Web3 and blockchain have yet to meet their expectations. What is the significance of Web3 and blockchain in the spatial web, and what will their influence be on the next generation of the internet? One of the objectives of Web3 is to establish an ecosystem that connects decentralized tools and applications. Web3 is powered by blockchain technology for cryptography. The security and verification of transactions can be done without the involvement of a central party, thanks to blockchain's immutability. Blockchain is built on coordination through a predefined set of rules.

The integration of geospatial data in Web 3.0 opens up a world of possibilities and challenges. Web 3.0 empowers us to build decentralized geospatial data infrastructures using blockchain technology and distributed ledger systems. These infrastructures offer the opportunity to securely store, share, and access geospatial data transparently while doing away with the reliance on centralized repositories and intermediaries.

The utilization of geospatial web technology plays a crucial role in driving major socioeconomic processes, empowering both experts and casual users with valuable insights to enhance their work, streamline daily tasks, and make well-informed decisions. Traditional workflows and practices are being transformed by innovative deep tech technologies across every industry sector. The widespread implementation of IoT, Big Data Analytics, Cloud Computing, Artificial Intelligence, and other technologies has been greatly facilitated by location intelligence solutions (Geospatial Media and Communications, 2019). While the potential of recent blockchain technology in leveraging geospatial applications remains underexplored, the announcement of the formation of a new Domain Working Group for Blockchain and Distributed Ledger Technologies (BDLT/DWG) by OGC in 2019 indicates a promising step forward.

The method efficiently divides encrypted information packets into several components, which are then incorporated into a spatial framework. The rapidly growing field of Spatial Data Encryption is being transformed by cutting-edge deep-tech innovations, causing major shifts in established processes and methodologies. In particular, the widespread adoption of technologies like IoT, Big Data Analytics, Cloud Computing, and Artificial Intelligence highlights the crucial need for enhanced data protection strategies. The security of network communications is the most significant issue in the world.

Information related to banks, credit cards, and government policies is transferred digitally from one location to another.

1.1 What is Crypto-Spatial?

Crypto-spatial represents the harmonious integration of blockchain technology and geospatial data, revolutionizing the management, sharing, and utilization of location-based information. Through inventive solutions harnessing the decentralized nature of blockchain networks, crypto-spatial enhances the security, integrity, and accessibility of geospatial data. Examples of these innovative solutions include:

1.1.1 Decentralized Spatial Data Infrastructure (SDI)

The utilization of blockchain-based SDI platforms allows for the establishment of decentralized networks that facilitate the storage, sharing, and access of geospatial data. Through distributed ledger technology, these platforms guarantee data integrity, immutability, and tamper resistance, thereby promoting trust among data providers and consumers.

1.1.2 Immutable Spatial Records

Geospatial data stored on blockchain networks is immutable, meaning it cannot be altered or deleted without the consent of network participants. This ensures that spatial information is reliable and trustworthy, making it ideal for applications requiring data provenance, such as land registry, supply chain tracking, and environmental monitoring.

1.1.3 Decentralized Spatial Marketplaces

Cryptospatial platforms allow users to buy, sell, or trade geospatial data, services, and applications using cryptocurrencies or digital tokens. Smart contracts oversee transactions, ensuring automated and transparent exchange of value between participants without the need for intermediaries.

1.1.4 Location-Based Services (LBS)

Blockchain-powered location-based service (LBS) platforms provide location-based services while safeguarding user privacy and data ownership. Users can securely share their location data with service providers or other users using encrypted protocols and have complete control over who can access their location information and for what purpose.

1.1.5 Geospatial Identity and Authentication

Blockchain technology enables the creation of decentralized identity systems that incorporate geospatial elements. This allows individuals or organizations to verify their position or closeness to certain geographical regions without exposing sensitive location information. These applications are particularly useful for controlling access, implementing virtual boundaries, and providing location-based services.

1.1.6 Geo-tagged Content and Applications

Cryptospatial platforms enable the development of geo-tagged content and applications that connect spatial information with blockchain transactions and smart contracts. This functionality allows developers to create location-based decentralized applications, games, social networks, and augmented reality experiences, making use of decentralized geospatial data sources..

1.1.7 Spatial Data Governance and Collaboration

Blockchain-based governance mechanisms enable decentralized decision-making and collaboration among stakeholders for managing and curating geospatial datasets. Smart contracts can enforce data sharing agreements, licensing terms, and data provenance requirements to ensure fair and transparent participation in spatial data ecosystems.

1.2 Need of the Geospatial data privacy

Protecting geospatial data privacy is crucial for a number of compelling reasons:

1.2.1 Protection of Personal Privacy

Geospatial data often includes individuals' locations, movements, and activities. Protecting this data is crucial to prevent unauthorized tracking or surveillance, which could lead to stalking, harassment, or other privacy invasions..

1.2.2 Prevention of Discrimination

Geospatial data can uncover sensitive information about individuals, including their socioeconomic status, ethnicity, and health conditions. Inappropriate use or exposure of this data could lead to discriminatory practices, such as targeted advertising or unfair treatment based on location or demographic characteristics.

1.2.3 Risk of Re-identification

When geospatial data is anonymized, it can still be linked with other data to identify individuals. This might inadvertently reveal people's identities or private information, which can compromise their privacy and confidentiality

1.2.4 Security Risks

Various sectors rely heavily on geospatial information, which is gathered and stored by diverse organizations, including governmental bodies, commercial enterprises, and independent data providers. It is imperative to implement strong security protocols to protect this information from potential unauthorized access, thereby safeguarding individuals against identity theft, fraudulent activities, and other security risks.

1.2.5 Trust and Consent

Respecting individuals' privacy rights is crucial for building trust and fostering positive relationships between data collectors and the public. It is essential to obtain informed consent and be transparent about the collection and use of geospatial data in order to maintain trust and ensure that individuals have control over their personal information.

1.2.6 Ethical Considerations

It's important to respect individuals' privacy, not just because it's the law, but also because it's the right thing to do. Organizations need to think about how their data collection and usage practices might affect people's privacy rights and make ethical choices in their decision-making processes.
Ensuring privacy of geospatial data is crucial for protecting individuals' rights, maintaining trust, and mitigating risks associated with location-based information collection, storage, and use.

2. Basic Knowledge

"Privacy-Preserving Spatial Data" refers to techniques and methodologies aimed at safeguarding the confidentiality and privacy of location-based information within geospatial datasets. As the collection and analysis of spatial data becomes more widespread in various applications, concerns about individual privacy and data protection have escalated. Ensuring the confidentiality of geospatial data is crucial for protecting sensitive information and maintaining the privacy rights of individuals and organizations.

"Geodata privacy" encompasses a set of principles and practices designed to safeguard the confidentiality of individuals, groups, communities, or organizations whose geographically specific data is collected for research, commercial, or other purposes (Keßler & McKenzie, 2018). This involves protecting data gathered by geospatial applications and services, such as Global Positioning System (GPS) tracking and location-based services, as well as data collection activities initiated by government, academic, commercial, or research organizations from unauthorized access, use, sharing, and disclosure. The term "geodata privacy" pertains to any privacy concerns arising from the sharing of geodata, which could lead to confidentiality breaches. It's important to note that geodata privacy violations may not always stem from ethical misconduct, but rather from a lack of knowledge or information.

It is essential to maintain the reliability, accuracy, and usefulness of geospatial data by ensuring its integrity. Organizations should implement strong data governance practices, quality assurance processes, data validation techniques, and security controls to accomplish this. Regular monitoring, auditing, and validation of data integrity are necessary to detect and address any issues promptly. Additionally, clear documentation, metadata standards, and data lineage tracking can help maintain transparency and accountability throughout the data lifecycle.

2.1 Geospatial data encryption requirement

“The issue of geospatial data privacy has gained increasing prominence in recent times. As location-enabled technologies and services such as Google Maps become more widespread, users are increasingly required to disclose their location to a growing number of external platforms” (Keßler and McKenzie, 2018). This proliferation of geospatial data sharing has sparked worries about potential threats to the privacy of users' location information.

“Protecting user privacy is the primary obstacle in geospatial data sharing, particularly for applications that utilize location information” (Zurbarán et al., 2018). Various forms of geospatial data can provide significant benefits to users and services. However, before disseminating this information, it is vital to implement privacy safeguards such as anonymization, perturbation, and encryption techniques.

In the last twenty years, numerous frameworks have been created to improve geoprivacy in the sharing of geospatial information. “These frameworks typically employ location obfuscation techniques, which are designed to protect privacy by intentionally decreasing the precision of location data to mask sensitive details, while still allowing the service to function effectively” (e.g., Partovi et al., 2020; Zurbarán et al., 2020; Hojati et al., 2021). As an example, Zurbarán and associates have substantially decreased the negative effects of location obfuscation on exploratory spatial data analysis (ESDA) through an algorithm known as Rand-K, which was introduced in 2018. Based on the research results, it is possible to minimize the algorithm's impact on spatial analysis.

2.2 Spatial data integrity

Throughout its lifecycle, geospatial data veracity ensures its accuracy, consistency, and reliability, crucial for maintaining its integrity and trustworthiness across various applications.

Make sure to set up strong data collection processes to guarantee that geospatial data is accurate and complete from the very beginning. This may involve using top-notch sensors, GPS devices, and surveying techniques, while also including quality control measures to identify and fix errors during data collection..

To ensure the quality of geospatial datasets, it is essential to include thorough metadata covering data sources, collection methods, accuracy assessments, and any data modifications. Detailed metadata empowers users to comprehend the data's context and limitations, fostering transparency and accountability.

Conduct thorough validation and quality assurance checks to ensure accuracy, consistency, and validity of geospatial data. This process includes conducting spatial and attribute checks, resolving inconsistencies or discrepancies, and verifying data against ground truth or reference datasets.

Incorporating version control mechanisms enables the tracking of changes and updates to geospatial datasets over time. It's important to maintain records of revisions, including details about the individuals who made the changes, the timing of the changes, and the reasons behind them. Regularly auditing and validating dataset versions is crucial for ensuring data integrity and traceability.

Geospatial data must be stored in highly secure and reliable repositories with robust access controls and encryption mechanisms to prevent any unauthorized tampering or alteration. Additionally, implementing backup and disaster recovery procedures is vital to ensure the prevention of data loss or corruption.

In order to facilitate seamless integration and exchange of geospatial data across different systems and platforms, it is essential to adhere to established data standards and interoperability frameworks. Consistent data formats, coordinate reference systems, and metadata conventions are crucial for promoting interoperability and mitigating the risk of data corruption or misinterpretation.

Let's establish robust policies and procedures for data governance, governing the collection, storage, sharing, and use of geospatial data. It's important to define the roles and responsibilities of data stewards and ensure their adherence to all relevant regulations and best practices for data integrity and security.

"Provide programs to educate and inform users and stakeholders involved in the management and use of geospatial data. Teach them about the importance of data integrity, best practices for data management, and the potential risks associated with data manipulation or misuse."

Organizations can implement specific strategies and take necessary steps to safeguard the integrity of their geospatial data. This approach will improve the data's dependability, practicality, and credibility for analytical purposes and decision-making processes. The quality and integrity of geospatial data play a vital role in the development and upkeep of spatial databases. Research conducted by Lin et al. in 2005 identified seven key elements of spatial data quality: lineage, positional accuracy, attribute accuracy, completeness, logic, semantic accuracy, and temporal information.

2.3 Ensuring the Confidentiality of Geospatial Data

To protect the integrity of geospatial data, organizations can utilize encryption techniques for secure storage and transmission. This ensures that the data remains unreadable in case of unauthorized access.

Ensure that strict access controls are in place to restrict individuals' ability to view or manipulate geospatial data. To achieve this, deploy rule-based access control (RBAC) and attribute-based access control (ABAC) mechanisms to ensure that specific datasets are only accessible to authorized individuals.

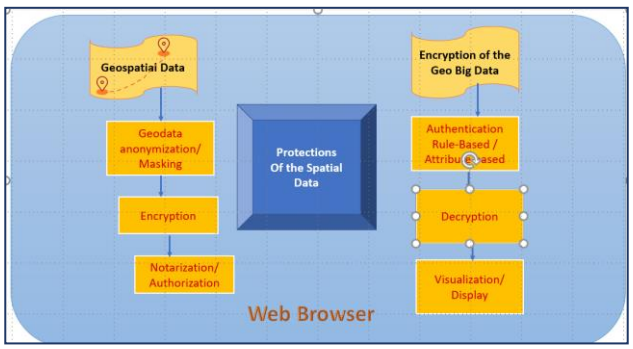

Figure 1: Rule/Attribute base Geodata Masking

Figure 1 has been determined to anonymize or pseudonymize sensitive location data to preserve the data's usefulness for analysis. This can be achieved through techniques such as generalization, suppression, and noise addition.

The act of masking involves safeguarding sensitive information in geospatial data by concealing certain sections. Blurring or pixelating specific areas in satellite imagery or maps can help prevent the identification of sensitive locations.

To maintain the security of geospatial data, it is important to store it in secure environments with robust access controls, and encryption, and conduct regular security audits to prevent unauthorized access to data at rest. When transmitting geospatial data across networks, ensure secure protocols such as HTTPS or VPNs are used to prevent interception or theavesdropping. Handling geospatial data requires careful management of associated metadata to ensure the protection of sensitive information. Whenever possible, it's best to limit the inclusion of detailed metadata or anonymize it.

It is crucial to adhere to the relevant legal frameworks and guidelines that govern the acquisition, utilization, and sharing of geospatial information. This encompasses following the European Union's GDPR, the United States' HIPAA, and India's policy on geospatial data usage.

Let's make sure to organize a training session for geospatial data handlers. During the session, we will cover topics such as confidentiality, best practices for handling data, and procedures for reporting security incidents.
It is important to consistently monitor access logs and perform regular audits to identify any suspicious activities. Any security breaches or unauthorized access should be promptly investigated and addressed.

3. Blockchain technology for geospatial data

Geo-blockchain, also referred to as spatial blockchain, represents a cutting-edge fusion of blockchain technology and geospatial data management systems. This novel approach extends beyond the traditional blockchain focus on transactions and smart contracts, enhancing blockchain capabilities to handle spatial data in a decentralized, transparent, and secure fashion. Through the implementation of distributed ledger technology, geo-blockchain safeguards the origin, accuracy, and protected storage of spatial information. As a result, this technology finds applications in diverse fields, such as supply chain logistics, land administration, and emergency response operations.

Geospatial data management stands to gain numerous advantages from the implementation of blockchain technology. This innovative approach offers a variety of potential uses, including strengthened data protection, enhanced traceability of data origins, distributed information sharing, and the enablement of direct spatial data transactions between parties.

3.1 Blockchain Technology for Spatial Data.

Fusing blockchain technology with geospatial technology offers valuable insights into this rapidly developing field's potential applications, challenges, and opportunities.

A significant point of discussion is the integration of blockchain with geospatial technology, highlighting potential benefits such as enhanced data security, improved data provenance, decentralized data management, and the facilitation of peer-to-peer transactions involving spatial data. Figure 2 explains how the Blockchain connects to the real-world representation of different departments compared to other databases, and how it

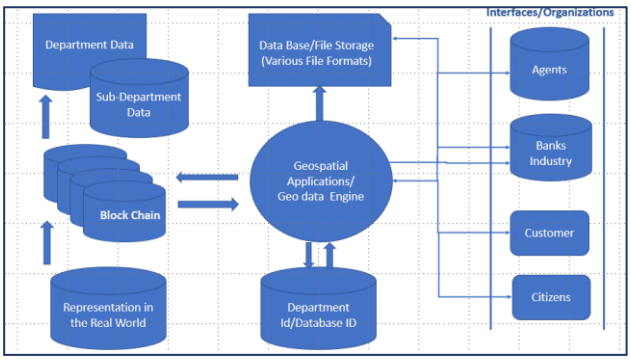

Figure 2 Ideal flow chart for Block chain for Geospatial Technology

can be beneficial to various organizations with their relational databases.

Review the existing literature and case studies on the applications of blockchain in geospatial technology across various domains.

- Land registration and property rights management
- Supply chain traceability and logistics
- Disaster management and humanitarian aid

- Environmental monitoring and conservation
- Location-based services and navigation
- Smart cities and urban planning

Let's consider the technical challenges and limitations associated with integrating blockchain with geospatial technology. These may include scalability, interoperability, data privacy, and consensus mechanisms. Additionally, let's discuss proposed solutions and approaches to address these challenges, such as sidechains, off-chain protocols, sharding, and privacy-preserving techniques.

Explore the security and trust implications of geospatial systems based on blockchain technology, including vulnerabilities, attack vectors, and potential threats. Discuss strategies for improving the security and trustworthiness of geospatial data on blockchain networks, such as cryptographic techniques, consensus mechanisms, and governance models.

Examine the significance of standards and interoperability frameworks in fostering the fusion of blockchain with geospatial technology. Explore initiatives aimed at establishing shared data formats, protocols, and interfaces for interconnected blockchain-based geospatial systems.

Delve into the regulatory and legal aspects linked to blockchain-based geospatial applications, encompassing data privacy regulations, intellectual property rights, jurisdictional matters, and liability considerations. Analyze the impact of regulatory frameworks such as GDPR and land tenure laws on blockchain-enabled geospatial systems.

Explore the latest trends, research gaps, and future paths for advancing the fusion of blockchain and geospatial technology. Delve into potential research areas, such as decentralized spatial data infrastructures, distributed geospatial analytics, and governance models for blockchain-based geospatial systems.

Summarize the essential findings and insights from the literature review, emphasizing the opportunities and challenges in harnessing blockchain technology for geospatial applications. Provide recommendations for future research and practical implications for policymakers, practitioners, and researchers in the field.

Researchers can enhance understanding, pinpoint research gaps, and inspire the creation of new solutions by thoroughly reviewing the literature on how blockchain can be integrated with geospatial technology. This is vital for progressing in this rapidly evolving interdisciplinary field.

3.2 Maintaining Data Accuracy and Unchangeability

The decentralized ledger structure of blockchain technology guarantees that geospatial information, once recorded, remains unalterable and tamper-proof without the agreement of network members. This feature safeguards the accuracy of data and blocks unauthorized changes to geographic details.

3.3 Data Provenance and Traceability

The transparent documentation of data exchanges, including the origin, background, and progression of geographic information datasets, is made possible through blockchain technology. This capability enhances the ability to trace data back to its source, thereby improving confidence and responsibility in the management of spatial data and related decision-making procedures.

3.4 Decentralized Data Sharing and Collaboration

Blockchain technology empowers decentralized data sharing and collaboration among multiple stakeholders in the geospatial domain. Through smart contracts, we can effectively govern data sharing agreements, access permissions, and data usage rights, ensuring a secure and transparent exchange of spatial information without the involvement of intermediaries

3.5 Secure Location-Based Services (LBS):

Blockchain-based location-based service (LBS) platforms can offer location-based services while ensuring user privacy and data ownership. Users can securely share their location data with service providers or other users using encrypted protocols, maintaining full control over who can access their location information and for what purpose.

3.6 Smart Contracts for Spatial Transactions

Self-executing agreements known as smart contracts, which are programmed on blockchain networks, have the ability to automate and enforce agreements related to geospatial transactions. For example, these contracts can automatically facilitate the transfer of real estate property ownership rights when specific conditions are met, such as payment completion and adherence to regulatory requirements.

3.7 Geo-Authentication and Geo-Signatures

Blockchain can be utilized to establish geo-authentication mechanisms that validate the authenticity and integrity of geospatial data. Geo-signatures, which are cryptographic proofs of location, can be stored on the blockchain to verify the origin and precision of spatial information, thereby increasing trust in spatial data sources.

3.8 Decentralized Spatial Data Marketplaces

Unlock the potential of blockchain-based platforms to facilitate decentralized marketplaces. Users can seamlessly buy, sell, or trade geospatial data, services, and applications using cryptocurrencies or digital tokens. Through smart contracts, transactions are securely governed, guaranteeing an automated and transparent exchange of value between participants, all without the need for intermediaries.

4. Web 3.0

The incorporation of geospatial data in Web 3.0 opens up a host of thrilling opportunities while also presenting some notable challenges.

4.1 Decentralized Geospatial Data Infrastructure

Web 3.0 paves the way for decentralized geospatial data infrastructures by leveraging blockchain technology and distributed ledger systems. These infrastructures offer a secure, immutable, and transparent framework for storing, sharing, and accessing geospatial data, presenting an opportunity to move away from centralized repositories and intermediaries.

4.2 Geo-enabled Smart Contracts

Smart contracts on blockchain platforms like Ethereum can be geo-enabled to execute location-specific transactions and agreements autonomously. For example, smart contracts can facilitate decentralized land registries, property transactions, and location-based services, ensuring transparency and trust in geospatial transactions.

4.3 Tokenization of Geospatial Assets

Web 3.0 allows for the tokenization of geospatial assets like land parcels, real estate properties, and environmental resources. This is done through the creation of cryptographic tokens on blockchain networks. These tokens represent fractional ownership, usage rights, or the origin of geospatial assets, making it possible for peer-to-peer trading, crowdfunding, and investment in these assets.

4.4 Decentralized Geospatial Marketplaces

Web 3.0 enables the development of decentralized geospatial marketplaces. In these marketplaces, users can directly buy, sell, or exchange geospatial data, services, and applications using blockchain-based payment systems. The platforms aim to establish fair and transparent pricing, encourage data sharing, and promote collaboration among participants in the geospatial ecosystem.

4.5 Privacy-Preserving Geospatial Analytics

Web 3.0 integrates privacy-preserving methods, including zero-knowledge proofs and decentralized computation. This allows for secure and private geospatial analytics without exposing sensitive location information. Users can conduct spatial analysis and gain insights from encrypted or anonymized geospatial data while safeguarding individual privacy and confidentiality.

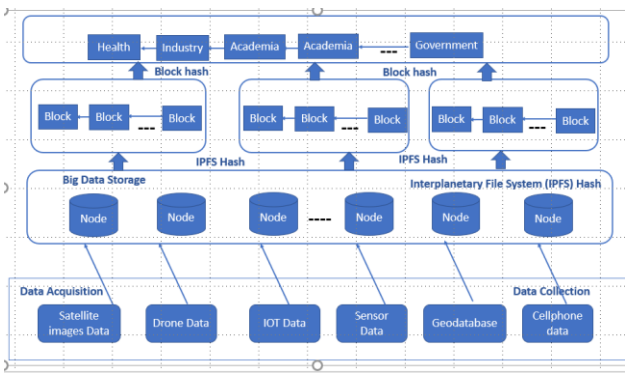

Figure 3 Flow chart with privacy of the data on Web3.0

Figure 3 illustrates how data moves from acquisition to storage, and then from storage to visualization and use at different levels and its privacy at different level.

4.6 Decentralized Geospatial Identity and Authentication

In the era of Web 3.0, decentralized identity management systems and geospatial authentication mechanisms are being introduced to empower individuals to securely control their location-based identities and access rights. Using decentralized identifiers (DIDs) and verifiable credentials, trusted geospatial authentication and authorization can be achieved across distributed networks.

4.7 Immutable Geospatial History and Provenance

Geospatial data stored on decentralized networks gains significant benefits from the immutability and provenance tracking provided by blockchain technology. This allows users to meticulously track the entire history of geospatial data changes, transactions, and validations, ensuring ironclad data integrity, audibility, and accountability in geospatial applications.

4.8 Interoperable Geospatial Standards and Protocols

Geospatial data stored on decentralized networks benefits from the immutability and provenance tracking provided by blockchain technology. Users can trace the entire history of geospatial data changes, transactions, and validations, ensuring data integrity, auditability, and accountability in geospatial applications.

5. Conclusion & Future

Studies and academic works confirm that geo-blockchain technology can substantially improve the integrity, security provenance, and decentralized storage of geographical data across diverse applications. This innovation facilitates the development of more reliable, transparent, and compatible geographical data systems, promoting efficiency and innovation in various sectors. By effectively tackling the unique challenges of spatial data management, geo-blockchain unveils a multitude of possibilities for exploring fresh perspectives and uses in the field of spatial data.

The potential of blockchain technology to transform the management, distribution, and use of geospatial data is immense, offering numerous chances for innovation, collaboration, and empowerment across different industries and applications. The implementation of Web 3.0, which utilizes blockchain technology, decentralized networks, and cryptographic methods, aims to establish a more transparent, secure, and collaborative geospatial ecosystem. By adopting decentralization and trustless systems, Web 3.0 introduces new opportunities for innovation, transparency, and democratization in the geospatial realm. However, it is crucial to tackle issues such as scalability, interoperability, and regulatory compliance to fully harness the potential of blockchain in the geospatial domain.

This study will undertake comprehensive research and practical experiments on the encryption and privacy protection of geospatial data using Web 3.0 technology. The main emphasis will be on safeguarding the privacy and integrity of geospatial data, particularly through blockchain technology in the context of smart cities and urban planning.

Acknowledgment

This work is an outcome of the project "Datasecurity4icity", a subproject of the project "ICity: Intelligent city" (https://www.hft-stuttgart.com/research/projects/i-city)". We extend our gratitude for the funding received through the FH-Impuls program under the number 13FH9E04IA by the German Federal Ministry of Education and Research (BMBF).

References

Amoretti, M., Brambilla, G., Medioli, F., and Zanichelli, F.: Blockchain-based proof of location, in: 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), pp. 146–153, IEEE, 2018.

Borges, K. A., Laender, A. H., and Davis Jr, C. A.: Spatial data integrity constraints in object oriented geographic data modeling, in: Proceedings of the 7th ACM international symposium on Advances in geographic information systems, pp. 1–6, 1999.

Chun, Y., Kwan, M.-P., and Griffith, D. A.: Uncertainty and context in GIScience and geography: challenges in the era of geospatial big data, 2019.

Coetzee, S., Ivánová, I., Mitasova, H., and Brovelli, M. A.: Open geospatial software and data: A review of the current state and a perspective into the future, ISPRS International Journal of Geo-Information, 9, 90, 2020.

Daho, A. B.: Crypto-spatial: an open standards smart contracts library for building geospatially enabled decentralized applications on the ethereum blockchain, The International Archives of Photogrammetry, Remote Sensing and Spatial Information Sciences, 43, 421–426, 2020.

Farnaghi, M. and Mansourian, A.: Blockchain, an enabling technology for transparent and accountable decentralized public participatory GIS, Cities, 105, 102 850, 2020.
Fecher, B. and Friesike, S.: Open science: one term, five schools of thought, in: Opening science, pp. 17–47, Springer, Cham, 2014.

Gordon, A. D. and Jeffrey, A.: Types and effects for asymmetric cryptographic protocols, Journal of Computer Security, 12, 435–483, 2004.

Hojati, M., Farmer, C., Feick, R., and Robertson, C.: Decentralized geoprivacy: leveraging social trust on the distributed web, International Journal of Geographical Information Science, 35, 2540–2566, 2021.

Huang, H., Yao, X. A., Krisp, J. M., and Jiang, B.: Analytics of location-based big data for smart cities: Opportunities, challenges, and future directions, Computers, Environment and Urban Systems, 90, 101 712, 2021.

Kamali, M., Malek, M. R., Saeedi, S., and Liang, S.: A Blockchain-Based Spatial Crowdsourcing System for Spatial Information Collection Using a Reward Distribution, Sensors, 21, 5146, 221.

Kamel Boulos, M. N., Wilson, J. T., and Clauson, K. A.: Geospatial blockchain: promises, challenges, and scenarios in health and healthcare, 2018.

Katsomallos, M., Tzompanaki, K., and Kotzinos, D.: Privacy, space and time: A survey on privacy-preserving continuous data publishing, Journal of Spatial Information Science, 2019, 57–103, 2019.

Keßler, C. and McKenzie, G.: A geoprivacy manifesto, Transactions in GIS, 22, 3–19, 2018.
Kitchin, R., Lauriault, T. P., and Wilson, M. W.: Understanding spatial media, Sage, 2017.

Kumar, K. M. and Sunitha, N.: Preserving Location Data Integrity in Location Based Servers using Blockchain Technology, in: 2017 2nd International Conference On Emerging Computation and Information Technologies (ICECIT), pp. 1–6, IEEE, 2017.

Lee, J.-G. and Kang, M.: Geospatial big data: challenges and opportunities, Big Data Research, 2, 74–81, 2015.

Leible, S., Schlager, S., Schubotz, M., and Gipp, B.: A review on blockchain technology and blockchain projects fostering open science, Frontiers in Blockchain, p. 16, 2019.

Lin, X., Zhang, Y., Liu, Y., and Gao, Y.: Spatial data integrity ensuring mechanism in SDBMS, in: Proceedings. 2005 IEEE International Geoscience and Remote Sensing Symposium, 2005. IGARSS’05., vol. 1, pp. 4–pp, IEEE, 2005.

Liu, P.: A survey of remote-sensing big data, frontiers in Environmental Science, 3, 45, 2015.

Lv, Z., Qiao, L., Hossain, M. S., and Choi, B. J.: Analysis of using blockchain to protect the privacy of drone big data, IEEE Network, 35, 44–49, 2021.

Lynch, S.: OpenLitterMap. com–open data on plastic pollution with blockchain rewards (littercoin), Open Geospatial Data, Software and Standards, 3, 1–10, 2018.

Martin, K. and Nissenbaum, H.: What is it about location?, Berkeley Tech. LJ, 35, 251, 2020.

Martin, M. E. and Schuurman, N.: Social media big data acquisition and analysis for qualitative GIScience: Challenges and opportunities, Annals of the American Association of Geographers, 110, 1335–1352, 2020.

Monrat, A. A., Schelén, O., and Andersson, K.: A survey of blockchain from the perspectives of applications, challenges, and opportunities, IEEE Access, 7, 117 134–117 151, 2019.

Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system, Decentralized Business Review, p. 21260, 2008.

Nofer, M., Gomber, P., Hinz, O., and Schiereck, D.: Blockchain, Business & Information Systems Engineering, 59, 183–187, 2017.

Papantoniou, C.: GeoBlockchain: The Analysis, Design, and Evaluation of a Spatially Enabled Blockchain, Ph.D. thesis, The Claremont Graduate University, 2021.

Papantonioua, C. and Hilton, B.: Workflows and Spatial Analysis in the Age of GeoBlockchain: A Land Ownership Example.
Partovi, A., Zheng, W., Jung, T., and Lin, H.: Ensuring privacy in location-based services: a model-based approach, arXiv preprint arXiv:2002.10055, 2020.

Pincheira, M., Donini, E., Giaffreda, R., and Vecchio, M.: A blockchain-based approach to enable remote sensing trusted data, in: 2020 IEEE Latin American GRSS & ISPRS Remote

Sensing Conference (LAGIRS), pp. 652–657, IEEE, 2020.
AGILE: GIScience Series, 3, 71, 2022 | https://doi.org/10.5194/agile-giss-3-71-2022 5 of 6

Qiu, Y., Liu, Y., Li, X., and Chen, J.: A novel location privacy preserving approach based on blockchain, Sensors, 20, 3519, 2020.
Sweeney, L.: k-anonymity: A model for protecting privacy, International Journal of Uncertainty, Fuzziness and Knowledge Based Systems, 10, 557–570, 2002.

Szabo, N.: Formalizing and securing relationships on public networks, First monday, 1997.

Tahiliani, A., Hassija, V., Chamola, V., Kanhere, S. S., Guizani, M., et al.: Privacy-preserving and incentivized contact tracing for covid-19 using blockchain, IEEE Internet of Things Magazine, 4, 72–79, 2021.

Tohidi, N. and Rustamov, R. B.: A review of the machine learning in gis for megacities application, Geogr. Inf. Syst. Geospat. Intell, pp. 29–53, 2020.

Vicente-Saez, R. and Martinez-Fuentes, C.: Open Science now: A systematic literature review for an integrated definition, Journal of business research, 88, 428–436, 2018.

Vos, J., Lemmen, C., and Beentjes, B.: Blockchain based land administration feasible, illusory or a panacea, in: Netherlands Cadastre, Land Registry and Mapping Agency. Paper prepared for presentation at the 2017 World Bank Conference on Land and Povertry. The World Bank, Washington, DC, 2017.

Xie, J., Tang, H., Huang, T., Yu, F. R., Xie, R., Liu, J., and Liu, Y.: A survey of blockchain technology applied to smart cities: Research issues and challenges, IEEE Communications Surveys & Tutorials, 21, 2794–2830, 2019.

Xu, H., Zhang, L., Onireti, O., Fang, Y., Buchanan, W. J., and Imran, M. A.: BeepTrace: blockchain-enabled privacypreserving contact tracing for COVID-19 pandemic and beyond, IEEE Internet of Things Journal, 8, 3915–3929, 2020.

Yaga, D., Mell, P., Roby, N., and Scarfone, K.: Blockchain technology overview, arXiv preprint arXiv:1906.11078, 2019.

Yang, M., Zhu, T., Liang, K., Zhou, W., and Deng, R. H.: A blockchain-based location privacy-preserving crowdsensing system, Future Generation Computer Systems, 94, 408–418, 2019.

Zhang, L., Gao, Y., Chen, J., Wang, X., Huang, Z., and Wei, D.: Research on Remote Sensing Data Sharing Model Based on Blockchain Technology, in: Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications, pp. 59–63, 2019.

Zhao, P., Bucher, D., Martin, H., and Raubal, M.: A clusteringbased framework for understanding individuals’ travel mode choice behavior, in: International Conference on Geographic Information Science, pp. 77–94, Springer, 2019.

Zurbarán, M., Wightman, P., Brovelli, M., Oxoli, D., Iliffe, M., Jimeno, M., and Salazar, A.: NRand-K: Minimizing the impact of location obfuscation in spatial analysis, Transactions in GIS, 22, 1257–1274, 2018.

Zurbarán, M. A., Salazar, A., Brovelli, M. A., and Wightman, P. M.: An evaluation framework for assessing the impact of location privacy on geospatial analysis, IEEE Access, 8, 158 224–158 236, 2020.

Webliography

https://agilegiss.copernicus.org/articles/3/71/2022/agile-giss-3-71-2022.pdf

www.int-arch-photogramm-remote-sens-spatial-inf-sci.net

www.kth.diva-portal.org