SUPREMO AMICUS

INDIA'S FIRST AI INTEGRATED LAW JOURNAL

Peer Reviewed, Refereed and Open access Journal

- Available in 331+ International Libraries
- Indexed at 32 Databases

ISSN NO. 2456-9704
Volume 10 Issue 1
www.supremoamicus.org

DISCLAIMER

The information presented in this article is intended for general informational and educational purposes only. While every effort has been made to ensure that the content is accurate, up-to-date, and reliable at the time of publication, the editorial board and publisher make no representations or warranties of any kind, express or implied, regarding the completeness, accuracy, reliability, suitability, or availability of the information contained herein.

The views and opinions expressed in this article are those of the author and are based on personal research, experience, and interpretation. They do not necessarily reflect the official policy, position, or opinions of any affiliated organization, institution, or entity.

This article is not intended to serve as professional advice of any kind. The editorial board and publisher shall not be held liable for any errors or omissions in the content, nor for any losses, injuries, or damages arising from the use of or reliance on this information.

ABOUT THE JOURNAL

Supremo Amicus is an online, peer-reviewed international journal devoted to the interdisciplinary fields of law and science. In an era marked by rapid technological progress and evolving legal frameworks, the journal seeks to bridge the gap between these two dynamic domains by offering comprehensive and critical insights into their various aspects. The journal places a strong emphasis on contemporary advancements, emerging trends, and the complex challenges faced by both the legal community.

The primary objective of the journal is to encourage and promote original, high-quality research. It is committed to publishing well-researched, analytically sound, and thought-provoking articles that adhere to rigorous academic standards. Each submission undergoes a thorough peer-review process to ensure authenticity, relevance, and scholarly integrity. In doing so, the journal maintains its commitment to excellence and credibility.

In addition to fostering research, the journal aims to make complex ideas accessible and engaging for a diverse readership. It strives to present content that is not only intellectually enriching but also clearly written and reader friendly.

Furthermore, the journal is committed to promoting interdisciplinary collaboration and global engagement. It welcomes diverse perspectives from contributors across different regions and backgrounds, thereby enriching the quality and scope of discussions presented within its pages.

With this vision we proudly present Supremo Amicus to our readers.

-Editorial Team
Supremo Amicus

RECONCILING THE IRRECONCILABLE: DATA PROTECTION AND THE IMMUTABLE LEDGER IN THE AGE OF BLOCKCHAIN

By *Sampurna Mishra*
Advocate & LLM, *Soa National Institute of Law*

Abstract:
Recent years have witnessed a rapid growth of blockchain technology which has revolutionized data storage, processing and governance in the digital economy. Although blockchain offers transparency, decentralization, and immutability, it also raises concerns about data protection and privacy. This study investigates the blockchain architecture and their compatibility with existing data protection regimes. It explores whether existing regimes can respond to the unique requirements posed by blockchain architecture.

This research mainly asks how data protection and privacy can be achieved in blockchain-based applications without spoiling the functionalities of this technology. This paper employs principally doctrinal and comparative research methods to respond this question. It examines key legal instruments such as the General Data Protection Regulation of the European Union and the Digital Personal Data Protection Act of India alongside emerging global regulatory approaches. The compatibility of blockchain with existing data protection principles such as the right to erasure, data minimisation, and purpose limitation will be examined in the light of secondary sources, namely academic literature, policy papers, and case studies.

According to the study, the immutability of Blockchain clashes directly with the right to be forgotten, a key element of recent data protection law. Furthermore, due to its decentralised and pseudonymous nature, it can be difficult to identify the controller and processors of data on blockchain. As a result, it complicates the allocation of legal liability. Nonetheless, the study outlines various solutions, including off-chain storage, encryption, zero-knowledge proofs, and permissioned blockchains, which may help solve these challenges. These innovations show that privacy and blockchain are not inherently incompatible; but rather require a re-evaluation of the design and regulation of both.

Since the research examines blockchain-related changes in legal norms and governance structures, it fits perfectly within the theme of the digital economy. In an increasingly decentralised world, this paper contributes to the ongoing debates about the future of data protection by addressing the clash between technological development and fundamental rights.

Keywords: Blockchain, Data Protection, Privacy, GDPR, Digital Economy

1. Introduction

Blockchain technology is rapidly expanding beyond a small-scale cryptographic experiment, into a foundation of decentralized systems, which can provide better data ownership, control, and interoperability in finance, healthcare, supply chain, and identity management. The basic innovations of blockchain that include immutability, transparency, and decentralization give unmatched assurances of data integrity and auditability. Such properties, in their turn, raise serious contradictions with the available data protection systems that primarily appreciate the rights of the individual, such as the right to erasure, the right to rectification and the right to purpose limitation.

The severity of the issue is great. By 2024, blockchain exploits had reached as much as $2.36 billion[1] and the first half of 2025 had surpassed 2.47.[2] Over three in every four of these attacks were attributed to hacked

1. Cyvers, *Security, Fraud, and Compliance Report 2024* (2024).

2. CertiK, *Hack3d: The Web3 Security Quarterly Report – Q2 + H1 2025* (2025).

privy keys and signature defects, which is to emphasize that the blockchain security remains a threat despite the enhancement of cryptography. Besides financial damages, the privacy cost is also very frightening: their transparency will make blockchain disclose transactional patterns and metadata of behaviour, as well as pseudonymous identities to more sophisticated deanonymization attacks.[3]

The following research question is the focus of this paper:

What is to be done to successfully redefine data protection and privacy as per blockchain architecture to reconcile the immutable transparency and individual privacy rights and compliance with regulations? To answer this question, the paper aims to achieve three purposes: the first one is to give a systematic mapping of the existing body of knowledge on the privacy issues of blockchain and privacy-saving solutions, the second one is to describe the gaps in the research field, which are yet to be filled, and the third is to offer the general design paradigm and practical recommendations of privacy-saving blockchain systems.

The paper will be structured in a way as follows. Section 2 discusses the pertinent literature in the fields of technical, legal and design. The research methodology is provided in Section 3. In sections 4 and 5, the research questions and gaps are mentioned. The analysis and synthesis of findings are provided in section 6. Section 7 gives recommendations to technologists, policymakers and researchers. Section 8 concludes with some restrictions and research directions.

2. Literature Review

2.1 The Immutability-Privacy Paradox

This is because the immutability of blockchain and the right to privacy are in inherent conflict, which the paper will call the immutability-privacy paradox. The European Union law, the General Data Protection Regulation (GDPR), provides the right of erasure (Article 17), rectification (Article 16), and restriction of processing (with the condition of the possibility to alter or delete the personal information) to the data subjects. Such modifications conflict with the inherent architecture of blockchain, namely, append-only, and the European Data Protection Board (EDPB) has acknowledged it. In April 2025 EDPB in its Guidelines 02/2025[4] made it clear that blockchain design should take into account the rights to access, rectification and erasure, and that blockchain and data protection were not the two opposite scenarios, but presented a challenge to organisations.

In a similar vein, the UK Information Commissioner's Office (ICO)[5] also conducted a consultation on distributed ledger technologies on the same date (in September 2025) and wrote that the nature of blockchain can make it difficult to execute individual rights, such as rectification and erasure, and offered the solution to this problem was to offer off-chain storage facilities so that data correction and erasure requests could be executed. The regulatory inclinations, which are described further, can be summarized as the following: the immutability-privacy paradox is not only a technical inconvenience but also a structural resistance necessitating significant alterations in the way blockchain architectures are treated.

3. Shan Wang et al., *Time Tells All: Deanonymization of Blockchain RPC Users with Zero Transaction Fee*, in Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security (2025).
4. European Data Protection Board, *Guidelines 02/2025 on Processing of Personal Data Through Blockchain Technologies* (Apr. 8, 2025).
5. Information Commissioner's Office, *Draft Guidance on Distributed Ledger Technologies* (Aug. 28, 2025).
6. California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100–1798.199 (West 2018).
7. Personal Information Protection Law of the People's Republic of China (2021).

2.2 Regulatory Frameworks: Comparative Analysis.

There is a high level of jurisdictional fragmentation in the regulatory environment of blockchain-based data processing. The strictest model is the GDPR, which emphasizes on the rights of the individual and the reduction of data. The 2025 guidelines of the EDPB support the idea that data protection by design is crucial and that the aspects of blockchain (such as immutability) must be supported by enhanced data protection by design at an early stage. The practical recommendations are as follows: Storing personal data on-chain when it is not needed and encryption, hashing and off-chain solutions to isolate personal data and immutable ledger records.

The patchwork of the sectoral and state-level regulations is used in the United States and the California Consumer Privacy Act (CCPA)[6] is the most comprehensive state-level regulation. The absence of federal privacy regulations has brought about the disintegration of regulations and it is now more difficult to comply with blockchain-based systems functioning across state borders. In the meantime, the Personal Information Protection Law (PIPL)[7] of China is following a different approach by focusing on the localization of the data as well as limitations on the transfer of data across the boundaries directly affecting blockchain-based models that imply the usage of globally distributed nodes.

This form of jurisdictional division, as one of the analyses has described it as a cause of geopolitical risks to the implementation of crypto, puts blockchain project activity in a gray area of compliance across a variety of jurisdictions. The absence of international consensus on the standards of privacy of blockchain is one of the greatest barriers to global implementation.

2.3 Privacy Threats and Attack Vectors.

Recent systematic reviews have conceptualized the privacy threats of different layers of blockchain systems. A 2025 systematic literature review recognizes privacy attack and protection at three distinct layers that include on-chain layer,[8] off-chain layer and infrastructure layer. On-chain attacks are transaction linking, dust attacks, and maximal extractable value (MEV) extraction, and each of them takes advantage of the transparent history of transactions on blockchain to deanonymize users and obtain value. Off-chain vulnerabilities comprise of failure of private key management and remote procedure call (RPC) exposure whereas infrastructure threats consist of signature hijacking and vulnerabilities of smart contracts.

Privacy attacks have continued to be successful, which is a pointer of the existence of these threats. The behavioral analysis used to correlate pseudonymous addresses, known as transaction linking attacks, is very effective even with the development of privacy-preserving technologies. The fact that more than 80 percent of the exploit losses arise because of the handling of the private keys characterizes a basic security vulnerability: the cryptographic guarantees are rendered useless whenever the key management practices are weak.[9]

2.4 Cryptographic Privacy Mechanisms

The 2025 literature records significant maturity in the cryptographic privacy mechanisms. One of the solutions that have become popular is Zero-Knowledge Proofs (ZKPs), which allow users to demonstrate the right to access or the validity of a transaction without disclosing any underlying private data. In a 2025 survey of ZKP implementations between 2021 and 2025, the authors found the most

8. F. A. Khan et al., *A Systematic Literature Review of Information Privacy in Blockchain Systems*, 5 J. Cybersecurity & Priv. 65 (2025).
9. T. Bayan et al., *Permissionless Blockchain Recent Trends, Privacy Concerns, Potential Solutions and Secure Development Lifecycle*, 17 Future Internet 547 (2025).
10. V. Sati, *Zero-Knowledge Proofs for Privacy-Preserving Systems: A Survey Across Blockchain, Identity, and Beyond* (July 15, 2025), https://zenodo.org/records/15917465.

frequently identified benefits,[10] barriers, and trends in the construction of privacy-preserving systems, including the fact that ZKPs have moved beyond academic projects and are now production infrastructure. They have been used to implement privacy-preserving on-chain permissioning of KYC-compliant decentralized apps, to combine Self-Sovereign Identity (SSI) with ZKPs to reconcile blockchain principles with regulatory compliance.

Similarly, Fully Homomorphic Encryption (FHE) has reached maturity and can now compute on encrypted data without decryption.[11] According to one 2025 industry analysis, in the year 2025, the encryption technologies such as Fully Homomorphic Encryption (FHE) and zero-knowledge proofs will have come out of academic theory and developed into commercial infrastructure. FHE has been integrated into blockchain systems by companies like Zama to raise large sums of money, and the technology space includes a variety of methodologies such as multi-party computation (MPC) and trusted execution environments (TEE).

The idea of Self-Sovereign Identity (SSI) frameworks has become popular as a paradigm of decentralized identity management. Decentralized Identity (DID)-based services based on the principles of SSI are becoming widely accepted as the basic technology that ensures the protection of personal data and provides users with the opportunity to manage their identities. On April 2025, the International Telecommunication Union (ITU-T) released Recommendation Y.3087 that defined functional requirements and architecture of blockchain-based self-controlled identity.[12] An example of a practical implementation of SSI is the YouGovern system, which runs on Binance Smart Chain but is based on W3C DID standards.

2.5 Privacy-by-Design Architectures

Privacy-by-design, which is an articulated principle in the GDPR under Article 25, has become especially relevant to blockchain systems. The guidelines of EDPB of 2025 underline that the data protection by design and default in accordance with Article 25 is especially critical to blockchain due to the difficulties that emerge in the implementation of the principles of data protection. Implementation should be done carefully, considerate and planned and with conscious application of technical protection mechanisms.[13]

The industry is moving to privacy-by-design architectures that combine encryption and selective disclosure. Analysis On the one hand, institutions can store immutable, auditable, golden record using encryption and selective disclosure as a 2026 analysis observes, and the real data remains hidden from competitors. An example of such a scheme is the Ptah framework, which has privacy-by-design on regulated tokenized asset networks, with each service in the architecture having controlled access to particular data.

3. Research Methodology

The paper utilizes a systematic literature review (SLR) methodology supported by the PRISMA 2020 principles, applied to the interdisciplinary scope of blockchain privacy research in computer science, law, and policy.

11. Zama Raises $57M in Series B to Bring End-to-End Encryption to Public Blockchains, THE BLOCK (June 25, 2025); Blockchain Privacy Revolution 2025: How Zama, Zcash, Aztec & zkVMs Are Redefining On-Chain Confidentiality, BITRUE (Oct. 18, 2025).
12. ITU-T, *Recommendation Y.3087: Self-Controlled Identity Based on Blockchain – Functional Requirements and Architecture* (Apr. 2025).
13. *Privacy by Design and Composability in Regulated Tokenized Asset Networks, BBCHAIN (June 25, 2025).*

3.1 Search Strategy

The search was done in academic databases such as IEEE Xplore, SpringerLink, ScienceDirect, PubMed, arXiv, and MDPI as well as regulatory repositories of GDPR, CCPA, and PIPL guidance documents. The search query was a combination of Boolean operators of three thematic groups:

- Blockchain terms: blockchain OR distributed ledger OR DLLT OR smart contract.
- Privacy terms: privacy and data protection or confidentiality or anonymity.
- Regulatory terms: GDPR OR compliance OR data protection by design OR right to erasure.

3.2 Inclusion and Exclusion Criteria.

To be included in the studies, they had to have: (i) been published between January 2023 and December 2025; (ii) covered the topic of privacy or data protection in blockchain environments; (iii) been peer-reviewed or official regulatory guidance; (iv) been written in English. The exclusion criteria included: (i) non-English literature; (ii) abstracts of conferences without full article; (iii) research on blockchain scalability or consensus mechanism excluding privacy considerations.

3.3 Data Extraction and Synthesis.

Out of a total population of 387 records, 71 studies were chosen and included in the study after elimination of duplicates and screening. Extracted data: (a) metadata of the publication; (b) research subject (technical, legal, design, or hybrid); (c) privacy threats identified; (d) solutions suggested; (e) regulatory frameworks discussed; (f) research gaps identified. They used thematic analysis to determine common patterns, tensions and solutions offered repeatedly throughout the literature.

4. Research Questions

The main and the secondary research questions discussed in this paper are as follows:

Primary Research Question:

RQ1: In what ways can data protection and privacy be successfully re-defined in blockchain systems to balance between the immutable transparency and privacy rights of individuals and compliance with regulatory obligations?

RQ2: Which are the leading technical and legal conflicts between blockchain immutability and data protection laws including GDPR, CCPA, and PIPL?

5. Identified Research Gaps

The systematic review exposes various research gaps that are consistent and need to be addressed by the scholars.

5.1 Gap 1: Privacy-by-Design in Permissionless Blockchain

Although regulatory guidance focuses on privacy-by-design, the literature does not specify any architectural patterns that would be used to implement these principles in permissionless (public) blockchain settings. Majority of the privacy-by-design frameworks are designed to run in permissioned blockchains where identity and access controls are centrally managed. The problem of selective disclosure and data minimization enforcement by full decentralization of permissionless networks is under-researched. Since one review observes, the formalisation of [cryptographic patterns] to blockchains into easily comprehensible design patterns to non-expert audiences is underdeveloped.

5.2 Gap 2: Cross-Jurisdiction Compliance Frameworks.

Although the issue of regulatory fragmentation has been acknowledged, there is still no detailed system of how to design blockchain systems that would be both GDPR, CCPA, and PIPL-compliant. The literature is inclined to concentrate on individual jurisdictions without comparative analyses to produce transferable design principles. There is no answer to the question of what data governance model (e.g., the data localization, cross-border data flow agreements) fits the distributed architecture of blockchain the best.

5.3 Gap 3: Scaling the Empirical Evaluation of Privacy Mechanisms.

Although cryptographic systems like ZKPs and FHE have shown theoretical potential, there is no empirical assessment of the mechanisms on a production scale in the literature. Laboratory benchmarks are reported in most studies, disregarding actual deployment metrics. The computational cost of ZKPs and FHE is still a limitation to widespread use, but there is little quantified trade-offs between privacy level, computational cost, and transaction throughput.

6. Findings and Analysis

6.1 The Immutability-Transparency Paradox as a Structural Paradox.

The analysis proves the fact that the dilemma between immutability of blockchain and rights of data protection is not solvable by technical means only but is a structural tension that needs to be addressed by both technical innovations and legal accommodation. The guidelines of EDPB 2025 recognise that blockchain and data protection are not antithetical concepts, but rather they represent a challenge to organisations, but it does not go as far as giving binding solutions. This uncertainty puts organizations in a compliance quandary especially when it comes to permissionless blockchains where no recognizable data controller can be identified, a situation that the GDPR fails to sufficiently address.[14]

The most acute conflict is the right to erasure. According to several regulatory reviews, the impossibility of the blockchain-based DLTs is inconsistent with the among others, right to erasure, rectification, and restriction of processing, as well as right to withdraw consent of the subjects of the data. The suggested workarounds, including off-chain storage of personal data and on-chain storage of only hashes, or the use of cryptographic redaction methods, partially address the regulatory need of deletion without trace, but not entirely.[15]

6.2 Cryptographic Mechanisms: Maturation and Persistent Barriers.

This is a period of significant cryptographic privacy maturation, spanning 2024 2025. ZKPs have also shifted to production infrastructure in finance, identity and healthcare applications. On-chain permissioning with SSI and ZKPs proves that the principles of blockchain can be used in line with regulatory compliance, allowing users to authenticate their access rights without disclosing any personal information.[16]

Nevertheless, there are still obstacles. ZKPs and FHE still impose computational overhead, which still curtails throughput in high-transaction settings. Although, ZK-rollups and zkVMs eliminate certain scalability issues, the privacy-performance dilemma is not a simple one. Also, the convoluted nature of cryptographic privacy features puts non-expert developers and users at an adoption disadvantage, which also plays into the existence of non-secure practices, including ineffective key management.[17]

6.3 Fragmentation and Compliance Costs.

The comparative analysis indicates that regulatory fragmentation also acts as a high compliance cost to blockchain projects that would want to have

14. *Interpreting the EDPB Draft Guidelines on Blockchain and Personal Data*, Canadian Web3 Council (July 8, 2025).
15. *Data Protection in Emerging Technologies: Blockchain*, DLA Piper (Nov. 14, 2022); *Adan's Response to the EDPB Consultation*, Adan (June 11, 2025).
16. *ZKP's $100M Privacy Framework*, Bitget News (Nov. 20, 2025); *Zero Knowledge Proof Market Size Report 2025-2033*, GII Research (Nov. 13, 2025).
17. Jiaxi Liu et al., *GENES: An Efficient Recursive zk-SNARK and Its Novel Application in Blockchain*, 14 Electronics 492 (2025).
18. *The Privacy Compliance Battle for Blockchain Companies*, Odaily News (Apr. 13, 2025); *A Batalha de Conformidade de Privacidade das Empresas de Blockchain*, Gate News (Apr. 13, 2025).

international deployment. The GDPR of the EU focuses on the rights of the individual and data minimization, the US has industry-specific and state-specific regulations with the CCPA being the most extensive, and the PIPL of China is characterized by localization of data and its regulation by the state.[18]
In the case of blockchain systems, such fragmentation results in irreconcilable demands. The right to erasure in GDPR is incompatible with immutability; the localization of data in PIPL is incompatible with distributed ledgers; and the decentralized approach of the US leads to jurisdictional ambiguity. One of the analyses notes that American companies would encounter a patching of rules that do not conform to the principles of free market and privacy. Lack of international standards - compatible to those that are developing around digital assets in frameworks such as MiCA - is a major gap in governance.[19]

7. Recommendations

This section gives concrete recommendations to three stakeholder groups, technologists and developers, policymakers and regulators, and researchers based on findings synthesis.

R1: Embrace Privacy-by-Design at the Design. The architectural design should be created to address privacy concerns and not afterwards. This includes: (i) off-chain storage of personal data where possible with on-chain hashes; (ii) selective disclosure (e.g., ZKPs), to limit data exposure; (iii) data minimization as a default, by storing no more data than is necessary to sustain a working system.[20]

R2: Case-based priority Cryptographic Privacy Mechanisms. Privacy mechanisms are not always adapted to all applications. ZKPs excel at verifying anonymously (e.g. KYC-compliant DeFi). It is possible to compute on encrypted data with FHE (e.g. confidential smart contracts). SSI with DID is the best identity management. Distributed key management and safe multi-party computation can be applied using MPC. Use-case-specific evaluations are something that developers ought to perform instead of going to a default mechanism.[21]

R3: Roll out Strong Key Management infrastructure. As over 80 percent of exploit losses are due to compromised personal keys, organizations can use: (i) multi-party computation (MPC), key management; (ii) key rotation and key revocation; (iii) key storage by their hardware security modules (HSMs) or trusted execution environments (TEEs); (iv) user education programs on good key management.[22]

R5: Build Internationalized Privacy Standards in Blockchain. Regulatory fragmentation that is present at the current time is a barrier to innovation and compliance. International bodies (e.g., ISO, ITU-T, G7, G20) should develop unified privacy standards in blockchain which should focus on fundamental principles, i.e., minimization of data, restrictions of its purpose and rights of individuals, and should be subject to the peculiarities of blockchain. The ITU-T Y.3087 recommendation on self-controlled identity models such standardization.[23]

R6: Privacy-Preserving Blockchain Innovation Regulatory Sandbox. Regulators should establish

19. Regulation (EU) 2023/1114 (MiCA), 2023 O.J. (L 150) 40.
20. EDPB Guidelines 02/2025 (Apr. 8, 2025); ICO Draft Guidance on DLT (Aug. 28, 2025)
21. IEEE (Nov. 2025) – ZKP+SSI for KYC DeFi; Bitrue (Oct. 18, 2025) – FHE; *Applied Sciences* 15(12):6437 (2025) – SSI; Volnov et al., *HOT Protocol* (arXiv, 2025) – MPC
22. Bayan et al., 17 *Future Internet* 547 (2025); Volnov et al., *HOT Protocol* (2025); Aildiz & Bahtiyar, *ACIT 2025 Conf. Proc.* 522 (IEEE 2025)
23. ITU-T Y.3087 (Apr. 2025); MiCA Regulation (EU) 2023/1114
24. Blockchain.News (Oct. 10, 2025); ICO Regulatory Sandbox (Oct. 1, 2025)

sandboxes to allow blockchain projects to experiment on their privacy-saving technologies under regulatory supervision to strike a balance between innovation and protection. The sandbox model would support: (i) test of innovative cryptographic protocols (e.g. ZKPs, FHE) to maintain regulatory compliance; (ii) best practices development of privacy-by-design in a blockchain; (iii) evidence-based policymaking relying on real-world deployment experience.[24]

8. Conclusion

The paper has discussed the intrinsic paradoxes between blockchain immutability and the rights to information protection, has conducted a systematic review of the 2024-2025 body of literature on blockchain privacy and has also offered an integrated strategy of re-evaluating data protection in a blockchain world. This review confirms that immutability-privacy paradox can no longer be solved in a technical context exclusively, but it requires concurrent cryptography, architecture, regulation, and human factors innovation.

The findings indicate that although cryptographic systems, particularly, ZKPs, FHE, and SSI have developed to a sophisticated stage, other barriers to mass adoption still exist, including the cost of computation, complexity, and regulatory fragmentation. Privacy exploits continue to cost dearly, and most of these exploits are because of human factors of big management than cryptographic vulnerability of over 80 percent. The privacy threat framework discussed in this paper leverages three layers that promote systematic vulnerability discovery on on-chain, off-chain and infrastructure layers.

The key conclusion is that blockchain and data protection are not two mutually exclusive phenomena that cannot be reconciled, but they can be reconciled with the help of consciously made decisions in design and transdisciplinary collaboration, as well as an openness to reconsider the technical design and regulatory frameworks in the context of a decentralized future.

*****