INATBA POSITION

by the PRIVACY WORKING GROUP

Leveraging Zero-Knowledge Proofs for GDPR Compliance in Blockchain Projects

October 2024

INATBA

International Association
for Trusted Blockchain Applications

Authors

Dave Zein, Block-Staff, Co-Chair of the Privacy Working Group, Czech Republic

Wiktor Pinkwart, token.com, Co-Chair of the Privacy Working Group, Poland

Reviewers

Catarina Silva, EUBOF Expert Group, Portugal

Geoffrey Goodell, INATBA Academic Advisory Body Member, UCL Blockchain, United Kingdom

Harris Niavis, Inlecom, Greece

Jonathan Heiss, INATBA Academic Advisory Body Member, TU Berlin, Germany

Jörn Erbguth, EUBOF Expert Group, Switzerland

Sharmin Chougule, INATBA Academic Advisory Body Member, University of Camerino, UNIDROIT, Italy

Sophoclis Stephanou, Blockchain.com, United Kingdom

Stéphanie Attias, The Sandbox, France

Table of Contents

As blockchain technology continues to mature, its core features - **immutability and transparency** - present obstacles for complying with modern privacy regulations, including the **General Data Protection Regulation (GDPR)**. The permanent and public nature of on-chain data, combined with blockchain's decentralized framework, creates challenges for developing blockchain-based or decentralized solutions in areas that involve personal data. **Zero-Knowledge Proofs (ZKPs)** offer a way to overcome these obstacles, enabling blockchain projects to meet GDPR requirements while preserving the benefits of decentralization. This paper explores the key benefits and potential applications of ZKPs in achieving GDPR compliance.

1. Understanding the GDPR Challenges

GDPR imposes a comprehensive set of obligations regarding the collection, storage, and processing of personal data. Key provisions, such as the **right to be forgotten** and **data minimization**, are particularly difficult to implement within blockchain's immutable structure. Once data is recorded on a blockchain, it cannot be easily altered or removed, which conflicts with GDPR's requirement that data be erased upon request.

Additionally, GDPR is developed on the premise of centralized entities acting as data controllers and data processors - roles that are ambiguous in decentralized systems. In blockchain, there is often no central authority responsible for managing personal data, making it challenging to assign accountability or ensure compliance. Moreover, blockchain's transparent nature, where data is shared across multiple nodes, complicates the **data minimization** principle, which requires that only the necessary amount of personal data be collected and shared. These structural differences underscore the difficulties of aligning blockchain technology with GDPR's privacy requirements.

2. Zero-Knowledge Proofs: A Solution

Zero-Knowledge Proofs (ZKPs) offer a practical method for addressing these privacy challenges in blockchain systems. ZKPs allow one party to prove to another that a statement is true without revealing any further information beyond the validity of the claim.

In a typical implementation, ZKPs generate a proof that can be hashed and stored on the blockchain, while the underlying data remains off-chain. This proof can be verified by the network without exposing any sensitive information. For example, a ZKP could prove that a user is over a certain age without revealing the user's exact birthdate. The cryptographic proof ensures that the verification is valid, but no personal data is shared or stored on the blockchain.

By limiting the exposure of personal information and reducing the amount of data stored on-chain, ZKPs help blockchain systems comply with GDPR's **data minimization** requirements. Additionally, ZKPs address the **right to be forgotten**

by ensuring that personal data remains off-chain, while only a hash of the data is stored on the blockchain. If a user requests their data to be erased, the cryptographic keys linked to the proof can be revoked or invalidated, rendering the proof unusable and ensuring that personal data becomes inaccessible. This approach allows blockchain to maintain its security and immutability while complying with GDPR's legal obligations.

3. Key Benefits of ZKPs for GDPR Compliance

3.1 Enhancing Data Privacy and Security of Personal Information

On-chain transparency, while beneficial for trust and decentralization, presents significant risks when it comes to handling personal data. The visibility of data across all network participants can increase the risk of unnecessary exposure and breaches, making it unsuitable for applications requiring privacy. Zero-Knowledge Proofs (ZKPs) provide a way to achieve privacy by allowing the validation of claims without revealing the underlying personal information.

By keeping sensitive data off-chain and only storing cryptographic proofs on the blockchain, ZKPs ensure that personal data is neither exposed nor vulnerable to unauthorized access or breaches. This system preserves the transparency and security of blockchain while protecting personal information, aligning with GDPR's privacy requirements.

3.2 Supporting Data Minimization

ZKPs help meet GDPR's **data minimization** requirement by ensuring that only the necessary information is processed and stored. When specific personal details are not needed for validation, they are neither collected nor retained. This reduces the data footprint on the blockchain, as only cryptographic proofs are stored, while sensitive data remains off-chain and is accessed only when required.

By minimizing the data stored and shared, ZKPs lower the risk of unnecessary exposure and ensure that blockchain systems process only essential information. This approach aligns with GDPR's principle of limiting data collection to what is strictly needed, protecting privacy while reducing the complexity of data handling in decentralized environments.

3.3 Enabling the Right to be Forgotten

Although blockchain's immutability poses challenges to data deletion, ZKPs can help by allowing data to be stored off-chain while only a hash of the data is kept on the blockchain. This hash can be rendered unusable if the data needs to be forgotten, thus complying with GDPR's right to be forgotten. By revoking the cryptographic keys or tokens linked to the zk-SNARKs, the system ensures that the proofs are no longer valid. This process ensures that personal data becomes inaccessible and effectively "erased" from a practical standpoint.

The concepts of ***Revocation of Proofs*** and ***Erasure Through Invalidation*** offer methods that can support blockchain's compliance with data protection standards, such as GDPR. These mechanisms allow for cryptographic proofs to be invalidated, ensuring that the associated data becomes inaccessible.

4. ZKPs in Blockchain Projects

Zero-Knowledge Proofs (ZKPs) have long been a focus of cryptographic research, but recent advancements have made their implementation more practical and accessible. With innovations such as **ZK Virtual Machines (ZK VMs)** and frameworks like **snarkJS** and **Circom**, the complexity of integrating ZKPs into blockchain environments has been significantly reduced. These tools streamline the process of generating zero-knowledge proofs by providing user-friendly interfaces and automating the conversion of higher-level code into the necessary proof structures.

4.1 Identity Verification and KYC

In the context of identity verification, ZKPs have potential to reshape the way **Know Your Customer (KYC)** processes are conducted. Traditional KYC systems require individuals to share personal information, such as identification documents, which introduces risks related to privacy breaches and identity theft. ZKPs enable the verification of personal credentials without revealing the underlying data, ensuring compliance with GDPR's data minimization principle.

Using ZKPs, an individual can prove attributes—such as being over 18 or holding citizenship—without exposing sensitive personal information. This cryptographic proof is generated on the user's device and can be validated by the verifier without accessing or storing personally identifiable information (PII).

Several companies are utilizing **ZKPs** to enhance identity verification and **KYC** processes in **Self-Sovereign Identity (SSI)** models. **Togggle** applies ZKP technology across various sectors, enabling users to verify credentials without exposing sensitive data. **zkMe** uses similar ZKP-based approaches to ensure private and decentralized identity verification. **Dock**, focusing primarily on healthcare, facilitates secure and private sharing of verifiable credentials in sensitive industries.

Self-Sovereign Identity (SSI) refers to an individual's control over their personal data, allowing them to manage and share it as they choose. While SSI often involves storing data locally on the user's device, it can also use decentralized or cloud-based storage, as long as the user retains full control over access and sharing.

By enabling individuals to retain control over their personal data while ensuring compliance with regulatory requirements, solutions like ZKP-based identity verification are setting new standards for secure and efficient KYC processes.

4.2 E-Voting Systems: Privacy Assurance through ZKP

Another significant application of ZKP is in **e-voting systems**, which require both transparency in the voting process and the confidentiality of individual voter preferences. ZKPs enable a system where voters can prove they have cast a valid vote without revealing their voting choice or personal identity. This ensures the integrity of the voting system while fully complying with data privacy laws.

ZKP-based e-voting systems work by generating proofs that can be verified without revealing the vote itself. The cryptographic protocols ensure that while the vote is validated, the system cannot trace the vote back to the voter, thereby maintaining both **anonymity and accountability**. For example, frameworks like **Trevo** have demonstrated how ZKP can be applied to voting systems by using blockchain for the transparent tallying and storage of votes together with ZKP for the verification of the voting process ensuring voter anonymity and ballot secrecy.

In the **Trevo framework**, ZKPs ensure that no unauthorized manipulation occurs in the voting process, while the decentralized ledger provides an immutable record of all transactions. By integrating smart contracts, Trevo also allows for the automatic tallying of votes and the execution of specific voting-related tasks, further enhancing the efficiency and trustworthiness of the process. This application demonstrates how ZKP can overcome the tension between transparency and privacy in blockchain-based voting.

4.3 Financial Applications & Privacy-Preserving Transactions

In the financial sector, **Zcash** offers a well-established example of how ZKPs can be used to enhance privacy while complying with regulatory frameworks such as GDPR. Zcash employs **zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge)** to allow for private cryptocurrency transactions. The use of zk-SNARKs enables Zcash users to send and receive funds without disclosing the transaction details to the public blockchain.

Theoretically, ZKPs in this context allow the verification of transactions—such as ensuring the validity of the amount sent—without exposing details about the sender, receiver, or the transaction value. This contrasts with transparent blockchains like Bitcoin, where all transaction details are publicly visible, making it difficult to maintain privacy.

In practice, Zcash offers two types of transactions: **transparent** and **shielded**. Transparent transactions function like typical public blockchain transactions, while shielded transactions leverage zk-SNARKs to ensure privacy. In a shielded transaction, Zcash hides the sender's address, receiver's address, and the transaction amount. This not only protects user privacy but also reduces the amount of data that is visible on-chain, supporting data minimization principles in line with the GDPR.

Selective Disclosure: Zero-Knowledge Proof-based architectures allow users to share specific transaction details with authorized third parties for auditing or compliance purposes. This ensures adherence to regulations such as Anti-Money Laundering (AML) while keeping personal data private by revealing only the necessary information.

Another noteworthy example of Zero-Knowledge Proof applications is ***Nightfall*** by **Ernst & Young (EY)**. *Nightfall* is an enterprise-grade privacy solution that uses zk-SNARKs to enable private token transfers on the public Ethereum blockchain. Like Zcash, *Nightfall* ensures transaction confidentiality while preserving the security and immutability of the blockchain.

Designed specifically for business-to-business (B2B) transactions, Nightfall addresses the crucial need for privacy to prevent the leaking of sensitive information to competitors. Its decentralized, autonomous authorization mechanisms allow enterprises to verify counterparties without revealing identities, thus supporting regulatory compliance without sacrificing privacy. This feature makes Nightfall particularly suitable for enterprises engaged in supply chain management, finance, and procurement, where the confidentiality of transaction data is essential.

Furthermore, Nightfall's open-source nature encourages wider adoption of privacy-preserving technologies across industries, providing enterprises with a robust and transparent tool for conducting private blockchain transactions while benefiting from the advantages of decentralization. For more details, visit EY's Nightfall page and the GitHub repository.

5. Conclusion

Zero-Knowledge Proofs represent a pivotal advancement in achieving GDPR compliance for blockchain projects. By ensuring data privacy, supporting data minimization, enabling the right to be forgotten, and enhancing scalability, **ZKPs provide a robust solution to the privacy and regulatory challenges posed by blockchain technology.** As the adoption of ZKPs continues to grow, blockchain projects can achieve the delicate balance between the transparency of decentralized systems and the privacy requirements of GDPR, paving the way for more secure and compliant blockchain applications.

6. References

European Union GDPR. (2018). General Data Protection Regulation (GDPR). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

Zcash Foundation. (2023). Zcash: Privacy-Preserving Cryptocurrency Using zk-SNARKs. Available at: https://z.cash/technology/

Dock. (2024). Decentralized Identity with Zero-Knowledge Proofs. Available at: https://www.dock.io/technology

Toggle. (2023). Leveraging ZKPs for Self-Sovereign Identity Verification. Available at: https://www.togggle.io/

Trevo. (2023). E-Voting with Privacy Using ZKPs. Available at: https://trustchain.ngi.eu/trevo/

Ernst & Young (EY). (2023). Nightfall: Privacy-Preserving Transactions for Enterprise-Grade Blockchain. Available at: https://blockchain.ey.com/technology | https://github.com/EYBlockchain/ZKPChallenge

Contact details

Website inatba.org

Contact contact@inatba.org

Join INATBA membership@inatba.org