# Protecting Your Digital Identity: The Revolutionary Potential of Zero-Knowledge Proof Encryption

BY MAURO LORENZO HALVE

The acceleration of digitalization has intensified concerns regarding data privacy, with data breaches becoming a common occurrence, and personal information being increasingly vulnerable to misuse. This article explores the escalating challenges posed by cyber threats, such as deepfakes and voice cloning, while highlighting the inadequacy of traditional encryption in a landscape where data compromise seems inevitable. It then introduces Zero-Knowledge Proof (ZKP), an advanced cryptographic protocol that offers a revolutionary solution by allowing data verification without revealing any underlying information. By explaining the potential of Zero-Knowledge Proof, the article emphasizes its significance in establishing a new paradigm for privacy, security, and compliance in the digital realm.

## Introduction

In our growing digital age, where every interaction and transaction leaves a digital footprint, the need for robust privacy solutions has never been more urgent. As cyber threats increase, data breaches become more common and with our data being collected by more and more corporations and governments, there is a growing unease about the security of personal information.

In the last couple of years both the public and private sector have encountered large-scale data breaches. Millions of fingerprints stolen in US government hack, 2015. Commissions on Elections data breach resulting in 55 million Philippine's personal data and voting activity, 2016. Biometric security firm Biostar' software leaked a million fingerprints and facial recognition data, 2019. Phone-numbers, birthdays, locations and other user records from Facebook were posted onto hacking forum, 553 million victims from 106 countries, 2021. Deutsche Bank, Commerzbank, ING and a dozen others' data breached in MOVEit Hack, 2023.

Whether the reason is fighting fraud or economic incentives, both the public and private sector are increasingly collecting, storing and using our (personal) data. For years, a data breach would result in some limited risks only. For example, victims of data breaches often get phone calls from exotic country codes or receive spam-mails from fake webshops.

Later, as a majority of people reuse passwords for everything, a data breach involving your email's password often offers hackers the opportunity to request a new password for other digital accounts, such as your bank, broker, or exchange account, resulting in those accounts being drained.

In other cases, hackers may obtain confidential business documents, personal identification documents, or photographs from your cloud provider allowing them to commit identity fraud, which in some cases is worse than financial damages.

Currently, with Artificial Intelligence and Unreal Engine (the most powerful real-time 3D creation tool for videogaming) also being adopted by bad actors, realistic deepfakes and voice cloning are becoming a dominant factor in today's attempts for fraud, scams, and blackmailing. These new inventions are increasingly fast, ever more deceiving and tailored using your own data against you. A deepfake clone of your boss asking you to transfer money, an AI-version of a well-known YouTuber with a fake give-away, a fake phone tap of a politician discussing to buy votes, and blackmailers using deepfake elicit content to extort victims; all in the news recently.

While on one hand fraud methods are getting more and more complex, the chances of falling victim are increasing and its implications are worsening, simultaneously a growing number of counterparties, from both the public and private sector, are collecting a wider reach of data. Due to this combination, as said, the need for robust digital privacy solutions has never been more urgent.

The question does not seem to be if your data will get leaked, but when your data will get leaked. As the databases holding our valuable information have proven to not always be as reliable as we would wish, the only solution seems to be to change the way they hold our data. A new type of encryption could potentially solve this.

## Encryption

Encryption is the cornerstone of data security. A practice rooted deeply in the archives of history, from ancient civilizations using basic substitution methods to mask their messages to modern-day enterprises employing complex algorithms to secure data. The essence of encryption remains consistent: converting information into an unreadable format to protect it from unwanted eyes.

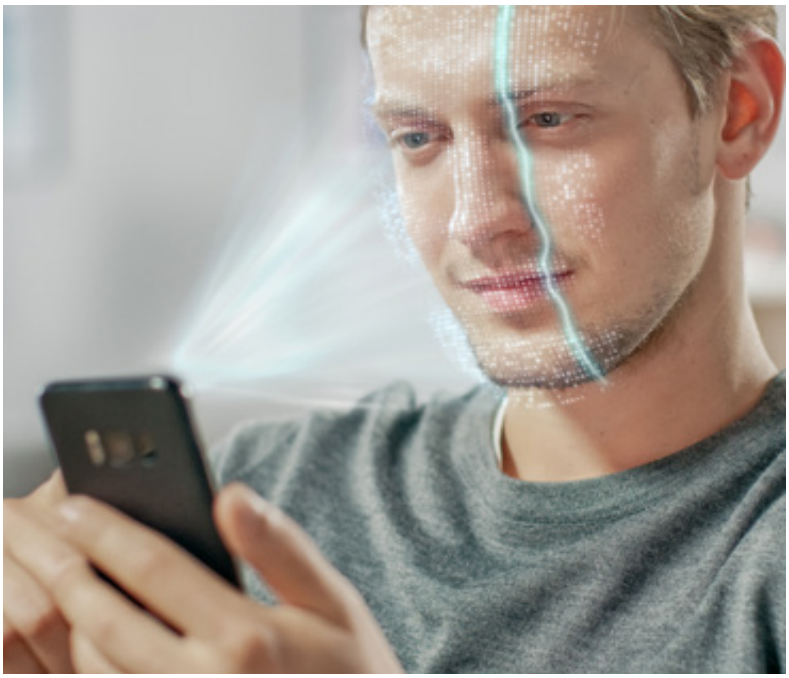
At its core, encryption is the process of transforming understandable data (plaintext) into an obscured format (ciphertext) using an algorithm and an encryption key. Only those possessing the corresponding decryption key can revert the ciphertext back to its original form, ensuring the data's confidentiality. In modern digital communications, encryption plays a pivotal role.

Whether it is safeguarding online transactions, protecting confidential emails, or securing sensitive files on a computer, encryption acts as the first line of defense against potential security breaches.

Nevertheless, while encryption offers robust security benefits, it is not without drawbacks. One of the primary disadvantages of encryption is the very essence of its purpose: it renders data unreadable. Therefore, data becomes unusable for sharing and using. While this is the intended outcome in many scenarios to protect sensitive data, it poses a challenge in situations where data needs to be accessible, useable, and/or verifiable.

For instance, you need to share (a picture of) your identity documentation for onboarding with a bank. Your document will – hopefully – be transmitted through encrypted communication channels. Nevertheless, as the bank needs to access and review your document, your data is not encrypted – only their database is. In essence, there is only a lock on their door. But once anyone has entry, all data is vulnerable. This highlights a critical aspect of encryption: while it secures data during transmission or at rest, it does not protect against vulnerabilities in security, negligence in access management, and carelessness with decryption keys, leading to potential breaches.

However, this could potentially become a thing of the past with the advent of innovative cryptography. One such breakthrough is the concept of Zero-Knowledge Proof (ZKP), a cryptographic protocol revolutionizing the way encrypted data can be used without decryption. This could be the first solution for transferring personal data while enhancing data security, safeguarding someone's privacy, and being able to comply with regulatory requirements at the same time.



## Zero-Knowledge Proof

Zero-Knowledge Proof is a cryptographic method of encryption, offering a new dimension of privacy, efficiency, and trust in digital interactions. It enables one party – known as the prover – to validate the truth of a statement towards another party – the verifier – without disclosing any underlying information about the statement itself. This ensures that sensitive data remains confidential, while still allowing for necessary verifications, allowing someone to digitally prove the truth of a statement without sharing the underlying data of the statement.

In more practical terms, consider the scenario of purchasing an exclusive bottle of wine on a website. If you would buy the wine in a store, the store's employee would confirm you are of legal age for buying alcohol. When buying the wine through the website and using Zero-Knowledge Proof, you could digitally verify you are of legal age without disclosing your date of birth nor any other personal information for that matter. Another example is to prove that you live in a specific area or country, without disclosing your private home address. Additionally, one could confirm to earn the necessary income for a mortgage or rent application, without revealing your exact salary and the unnecessary personal information on your pay slip.

The concept of Zero-Knowledge Proof was first introduced by three MIT computer scientists: Shafi Goldwasser, Silvio Micali, and Charles Rackoff in their seminal paper, "The Knowledge Complexity of Interactive Proof Systems." This groundbreaking work laid the foundation for Zero-Knowledge Proof by establishing a method where one could prove the validity of a statement without communicating any additional information beyond the fact that the statement was true or false. The concept was initially a theoretical construct, intriguing mathematicians and cryptographers with its potential.

Over the decades, the concept of Zero-Knowledge Proof remained present in the field of academic research, with various protocols and Proofs being developed to expand its efficiency and applicability. Among those was a paper by the brilliant cryptographer and computer scientist Hal Finney.

As the digital age progressed, the need for practical applications of Zero-Knowledge Proof became more obvious, with privacy concerns growing with the increasing exchange of digital data. But it was not until the rise of blockchain technology, in which Hal Finney also played a dominant role, and the associated need for enhanced privacy measures that Zero-Knowledge Proof began to

see real-world implementation on a significant scale. Blockchain's inherent properties of decentralization, immutability, and transparency provided a fertile ground for Zero-Knowledge Proof to solve the apparent paradox of sharing information securely without actual data transfer. Zero-Knowledge Proofs has been implemented into various blockchains and cryptocurrency protocols, providing users with the ability to conduct transactions and prove credentials without exposing any underlying private information.

Innovations such as zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) have further propelled the technology into the spotlight. Succinct refers to a smaller size of proof and, unlike traditional Zero-Knowledge Proofs, zkSNARKs are non-interactive, meaning the prover and the verifier only need to exchange a single argument. This allows for faster and more efficient proofs without the need for interaction between the prover and verifier.

In my opinion, the most interesting is the concept of zkKYC: a solution concept for KYC without knowing your customer, leveraging the combination of self-sovereign identities and zero-knowledge proofs. Know Your Customer (KYC) processes are essential nowadays, mainly within the financial sector. They help companies verify the identity of their customers, ensuring transparency and compliance with regulations and minimizing fraud risks. Traditional KYC methods often require collecting detailed personal information, which can be at risk if the company's data storage is compromised.

This innovative approach offers numerous advantages. It enhances privacy, as individuals are no longer required to expose their personal details. Complementary, it ensures regulatory compliance and reduces the likelihood of fraud, as businesses can verify client information without accessing the actual data. Lastly, the process becomes more efficient and cost-effective, eliminating the need to transfer, store, and manually verify sensitive information.

As we continue to navigate through an era dominated by digital interactions, the demand for secure and private systems is on the rise. The adoption of blockchain technology and advanced cryptographic methods like ZKP is a promising step toward a future where personal data is protected, and identity verification is secure, efficient, and user-friendly. This evolution in digital security paves the way for a digital ecosystem where cryptographic assurances safeguard our information, fostering a safer and more private digital world for all.

**Mauro Lorenzo Halve**
Digital Assets, Compliance & AML, CCPC, CBP, CEP, Senior Compliance Officer at Amdax

Mauro has a passion for compliance and cryptocurrency. He works as a senior compliance officer for **Amdax**, a digital asset custodian and wealth manager in Amsterdam. After his first introduction with bitcoin in early 2017 during law school, there has not been a day without reading about bitcoin or any related topic. Mid-2019 he founded his own crypto company, providing asset management for private clients, which he successfully sold in 2021 to the company he started to work for in 2020, as the compliance officer. In 2022, he was the project lead obtaining the Dutch crypto service provider license for said company and was appointed as Chief Compliance Officer and approved by the Dutch Central Bank. In February 2023, he made the transition to Amdax, the leading digital asset house of the Netherlands.