SEBA BANK

August 2023

Zero-Knowledge Guardian of Privacy

The Bridge

Your Regulated Global Crypto Bank

Table of Contents

Author

Rishabh Nagar
Research Analyst
SEBA India

Contact

research@seba.swiss

Introduction

In a world where information is both a valuable asset and a vulnerable liability, where digital connections weave intricate webs of transactions, interactions, and communications, a groundbreaking concept has emerged – a concept that promises to turn the tables on invasive surveillance, data breaches, privacy concerns and a profound impact that resonates strongly with cryptocurrencies. Welcome to the enigmatic realm of Zero-Knowledge Proofs (ZKPs), where cryptographic magic unveils itself and information becomes an impenetrable fortress.

Imagine a world where you can validate claims, authenticate identities, and conduct transactions, all while keeping your secrets hidden from prying eyes. ZKPs offer an unprecedented solution, allowing you to unlock the power of verification without revealing more than necessary. It's like playing an exhilarating game of wits, where you prove your knowledge without divulging the underlying secrets.

In a domain characterized by decentralized ledgers, digital transactions, and the very essence of trust in a virtual realm, ZKPs offer a potent remedy. They redefine how privacy can coexist harmoniously with transparency, paving the way for a new standard in secure transactions. This cryptographic marvel is the linchpin in the wheelwork of the blockchain revolution – a testament to the transformative power of innovation and the ingenuity of the human mind.

Together, we will embark on a thrilling journey through the intricate mechanisms of ZKPs. We will unravel the mystique behind their impeccable security and privacy preservation. From protecting personal information to revolutionizing digital trust in the banking sector, ZKPs have emerged as the mighty guardians of privacy, reshaping the very fabric of our interconnected world.

Join us as we delve into the mesmerizing world of ZKPs, where information becomes power and privacy becomes invincible.

Zero-Knowledge Proof in simple words

Today, we are going on an exciting journey to discover “Zero-Knowledge Proofs”. Don’t worry if it sounds complicated; we will ensure it’s as fun and easy to understand as a puzzle game! Are you ready? Let’s dive in!

Zero-Knowledge Proof Game?

Imagine you and your friend find a mysterious treasure chest that can only be opened with a secret password. You both want to know if you have the right password without revealing it to each other. That’s when Zero-Knowledge Proofs come to the rescue!

The Magical Puzzle

You and your friend will pretend to be two detectives to play this game. You’ll have a special puzzle with hidden clues. The goal is to prove that you know the secret password without telling it to your friend. It’s like showing them a magic trick, but they can’t figure out how you did it!

The Detective’s Game

Let’s pretend you are the detective and your friend is the treasure chest guardian. You’ll start by taking turns. On your turn, you’ll show your friend a piece of the puzzle without revealing the whole picture. Your friend can sift through it, but they won’t be able to guess the password based on that one piece.

The Magic Continues

You and your friend will keep taking turns showing different puzzle pieces each time. But here’s the clever part: always ensure that each puzzle piece you show can only be understood if you know the secret password. It’s like you’re giving your friend a new piece of the puzzle every time, but they still can’t figure out the whole picture!

The Exciting Revelation

After several turns, something amazing will happen. Your friend, the treasure chest guardian, will suddenly realize that you must know the secret password. How? Because you’ve shown them so many puzzle pieces that fit perfectly together, and it’s impossible for you to do that unless you truly know the secret! It’s like they can see the whole picture now, even though you never told them the password.

The Trustworthy Proof

At the end of this fun game, your friend will have absolute confidence that you know the secret password, even though they have no idea what it actually is. This is how Zero-Knowledge Proofs work! You’ve proven your knowledge of the password without revealing it, and your friend trusts you completely.

Congratulations, detective! You’ve learned about ZKPs and mastered the art of proving something without giving away the secret. Like in our puzzle game, ZKPs allow us to verify information without revealing all the details. Remember, secrets can be fun, but sometimes it’s important to prove what we know without sharing everything. Great job!

I believe we are now well equipped to give a try to understand Zero-Knowledge Proofs in a formal setting – The Internet way.

What are Zero-Knowledge Proofs, and how does it work?

Zero-Knowledge Proofs (ZKPs) are cryptographic protocols that allow one party, known as the prover, to prove to another party, called the verifier, that a specific statement is true without revealing any additional information about the statement. The concept was introduced in the 1980s by Shafi Goldwasser, Silvio Micali, and Charles Rackoff in the paper The Knowledge Complexity of Interactive Proof Systems.

The primary goal of a Zero-Knowledge Proof is to convince the verifier of the validity of a statement while disclosing no information other than the statement's truthfulness. This property makes ZKPs useful in various applications where privacy, security, and authentication are essential.

To understand how ZKPs work, let's break down the process into its fundamental components:

Statement

A ZKPs starts with a statement the prover wants to prove to the verifier. The statement can be any claim or assertion the prover wants to demonstrate as true. For example, it could be "I possess a secret key" or "I know a solution to a mathematical problem".

Proof Generation

During the protocol, the prover constructs a proof based on their knowledge of the statement's truth. This proof is designed in such a way that it convinces the verifier without revealing any confidential information.

Verification

The verifier examines the proof provided by the prover to determine its validity. The verifier's goal is to ensure that the proof is convincing enough to demonstrate the truthfulness of the statement.

Soundness

A crucial aspect of ZKPs is soundness. It guarantees that an honest verifier will only be convinced if the statement is true. The prover cannot convince the verifier to believe a false statement to be valid.

Zero-Knowledge Property

The most significant aspect of ZKPs is their Zero-Knowledge Property. It means that the proof does not reveal any additional information about the secret knowledge the prover possesses apart from the statement's truth. The verifier gains confidence in the statement without learning anything else.

Conclusion

In an era dominated by data-driven technologies and growing privacy concerns, ZKPs have emerged as a game-changing concept. They offer a robust solution to protect privacy, enhance security, and establish trust without unnecessary disclosure of sensitive information. From financial transactions to identity verification and secure computations, ZKPs empower individuals and organizations to navigate the digital landscape confidently. As we progress, the continued development and implementation of ZKPs will be crucial in preserving privacy, strengthening security, and fostering trust in our increasingly interconnected world.

In part 2 of the Zero-Knowledge series, we will try to deep dive into ZKPs and give you a holistic understanding of how different types of ZKPs, such as a SNARK or a STARK, work, which one is better, use cases and how ZKPs can help in saving us from the haunting of quantum computers.

Preserving privacy and strengthening security: Why do we need Zero-Knowledge Proofs?

In today's interconnected world, where privacy breaches and security threats loom, finding innovative solutions that protect sensitive information while establishing trust has become paramount. One such groundbreaking solution is the concept of ZKPs. ZKPs offers a way to prove a statement's truth without divulging additional information. This section will explore why ZKPs are crucial in various domains and how they reshape privacy, security, and trust in our digital landscape.

Protecting Privacy

Privacy has become a precious commodity in the digital age. Individuals are increasingly concerned about safeguarding sensitive information, from online transactions to personal communications ZKPs provide a powerful tool for preserving privacy. They enable individuals to prove the validity of a claim or statement without disclosing unnecessary details, ensuring that only essential information is shared. This is particularly vital in domains like financial transactions, where privacy is a cornerstone, and in authentication protocols, where personal information needs to be protected.

Enhancing Security

Security breaches and unauthorized access to sensitive data pose significant threats today. ZKPs play a pivotal role in strengthening security measures. By allowing individuals to prove their knowledge or authorization without explicitly revealing confidential information, ZKPs mitigate the risk of data breaches and fraudulent activities. Applications such as cryptographic systems and secure computations benefit greatly from ZKPs, as they enable secure operations on encrypted data, protecting against malicious attacks and ensuring data integrity.

Building Trust and Verification

Trust is the foundation of many interactions, whether in business transactions, audits, or voting systems. ZKPs offer a way to establish trust without complete disclosure. They allow one party to prove the truthfulness of a claim to another party without revealing any additional information beyond the claim's validity. This enhances transparency while maintaining confidentiality, ensuring that parties can verify each other's assertions without compromising sensitive data. ZKPs provide a robust mechanism for identity verification, access control, and secure computations, bolstering trust in various applications.

Empowering Blockchain and Cryptocurrencies

The rise of blockchain technology and cryptocurrencies has brought forth new challenges in terms of privacy and security. ZKPs have emerged as a powerful tool to address these challenges. They enable privacy-preserving transactions on the blockchain, concealing transaction details such as the sender, recipient, and amount while ensuring the transaction's validity. This breakthrough has significant implications for financial privacy, business confidentiality, and the widespread adoption of digital currencies, where maintaining transaction privacy is crucial.

Disclaimer

This document has been prepared by SEBA Bank AG ("SEBA") in Switzerland. SEBA is a Swiss bank and securities dealer with its Head Office and legal domicile in Switzerland. It is authorized and regulated by the Swiss Financial Market Supervisory Authority (FINMA). This document is published solely for information purposes; it is not an advertisement nor is it a solicitation or an offer to buy or sell any financial investment or to participate in any particular investment strategy. It is not directed to, or intended for distribution to or use by, any person or entity who is a citizen or resident of or located in any locality, state, country or other jurisdiction where such distribution, publication, availability or use would be contrary to law or regulation or would subject SEBA to any registration or licensing requirement within such jurisdiction.

No representation or warranty, either express or implied, is provided in relation to the accuracy, completeness or reliability of the information contained in this document, except with respect to information concerning SEBA. The information is not intended to be a complete statement or summary of the financial investments, markets or developments referred to in the document. SEBA does not undertake to update or keep current the information. Any statements contained in this document attributed to a third party represent SEBA's interpretation of the data, information and/or opinions provided by that third party either publicly or through a subscription service, and such use and interpretation have not been reviewed by the third party.

Any prices stated in this document are for information purposes only and do not represent valuations for individual investments. There is no representation that any transaction can or could have been effected at those prices, and any prices do not necessarily reflect SEBA's internal books and records or theoretical model-based valuations and may be based on certain assumptions. Different assumptions by SEBA or any other source may yield substantially different results.

Nothing in this document constitutes a representation that any investment strategy or investment is suitable or appropriate to an investor's individual circumstances or otherwise constitutes a personal recommendation. Investments involve risks, and investors should exercise prudence and their own judgment in making their investment decisions. Financial investments described in the document may not be eligible for sale in all jurisdictions or to certain categories of investors. Certain services and products are subject to legal restrictions and cannot be offered on an unrestricted basis to certain investors. Recipients are therefore asked to consult the restrictions relating to investments, products or services for further information. Furthermore, recipients may consult their legal/tax advisors should they require any clarifications. SEBA and any of its directors or employees may be entitled at any time to hold long or short positions in investments, carry out transactions involving relevant investments in the capacity of principal or agent, or provide any other services or have officers, who serve as directors, either to/for the issuer, the investment itself or to/for any company commercially or financially affiliated to such investment.

At any time, investment decisions (including whether to buy, sell or hold investments) made by SEBA and its employees may differ from or be contrary to the opinions expressed in SEBA research publications.

Some investments may not be readily realizable since the market is illiquid and therefore valuing the investment and identifying the risk to which you are exposed may be difficult to quantify. Investing in digital assets including crypto assets as well as in futures and options is not suitable for every investor as there is a substantial risk of loss, and losses in excess of an initial investment may under certain circumstances occur. The value of any investment or income may go down as well as up, and investors may not get back the full amount invested. Past performance of an investment is no guarantee for its future performance. Additional information will be made available upon request. Some investments may be subject to sudden and large falls in value and on realization you may receive back less than you invested or may be required to pay more. Changes in foreign exchange rates may have an adverse effect on the price, value or income of an investment. Tax treatment depends on the individual circumstances and may be subject to change in the future.

SEBA does not provide legal or tax advice and makes no representations as to the tax treatment of assets or the investment returns thereon both in general or with reference to specific investor's circumstances and needs. We are of necessity unable to take into account the particular investment objectives, financial situation and needs of individual investors and we would recommend that you take financial and/or tax advice as to the implications (including tax) prior to investing. Neither SEBA nor any of its directors, employees or agents accepts any liability for any loss (including investment loss) or damage arising out of the use of all or any of the Information provided in the document.

This document may not be reproduced or copies circulated without prior authority of SEBA. Unless otherwise agreed in writing SEBA expressly prohibits the distribution and transfer of this document to third parties for any reason. SEBA accepts no liability whatsoever for any claims or lawsuits from any third parties arising from the use or distribution of this document.

Research will initiate, update and cease coverage solely at the discretion of SEBA. The information contained in this document is based on numerous assumptions. Different assumptions could result in materially different results. SEBA may use research input provided by analysts employed by its affiliate B&B Analytics Private Limited, Mumbai. The analyst(s) responsible for the preparation of this document may interact with trading desk personnel, sales personnel and other parties for the purpose of gathering, applying and interpreting market information The compensation of the analyst who prepared this document is determined exclusively by SEBA.

Austria: SEBA is not licensed to conduct banking andfinancial activities in Austria nor is SEBA supervised by the Austrian Financial Market Authority (Finanzmarktaufsicht), to which this document has not been submitted for approval. France: SEBA is not licensed to conduct banking and financial activities in France nor is SEBA supervised by French banking and financial authorities. Italy: SEBA is not licensed to conduct banking and financial activities in Italy nor is SEBA supervised by the Bank of Italy (Banca d'Italia) and the Italian Financial Markets Supervisory Authority (CONSOB - Commissione Nazionale per le Società e la Borsa), to which this document has not been submitted for approval. Germany: SEBA is not licensed to conduct banking and financial activities in Germany nor is SEBA supervised by the German Federal Financial Services Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht), to which this document has not been submitted for approval. Hong-Kong: SEBA is not licensed to conduct banking and financial activities in Hong-Kong nor is SEBA supervised by banking and financial authorities in Hong-Kong, to which this document has not been submitted for approval. This document is not directed to, or intended for distribution to or use by, any person or entity who is a citizen or resident of or located in Hong-Kong where such distribution, publication, availability or use would be contrary to law or regulation or would subject SEBA to any registration or licensing requirement within such jurisdiction. This document is under no circumstances directed to, or intended for distribution, publication to or use by, persons who are not "professional investors" within the meaning of the Securities and Futures Ordinance (Chapter 571 of the Laws of Hong Kong) and any rules made thereunder (the "SFO"). Netherlands: This publication has been produced by SEBA, which is not authorised to provide regulated services in the Netherlands. Portugal: SEBA is not licensed to conduct banking and financial activities in Portugal nor is SEBA supervised by the Portuguese regulators Bank of Portugal "Banco de Portugal" and Portuguese Securities Exchange Commission "Comissao do Mercado de Valores Mobiliarios". Singapore: SEBA is not licensed to conduct banking and financial activities in Singapore nor is SEBA supervised by banking and financial authorities in Singapore, to which this document has not been submitted for approval. This document was provided to you as a result of a request received by SEBA from you and/or persons entitled to make the request on your behalf. Should you have received the document erroneously, SEBA asks that you kindly destroy/delete it and inform SEBA immediately. This document is not directed to, or intended for distribution to or use by, any person or entity who is a citizen or resident of or located in Singapore where such distribution, publication, availability or use would be contrary to law or regulation or would subject SEBA to any registration or licensing requirement within such jurisdiction. This document is under no circumstances directed to, or intended for distribution, publication to or use by, persons who are not accredited investors, expert investors or institutional investors as declned in section 4A of the Securities and Futures Act (Cap. 289 of Singapore) ("SFA"). UK: This document has been prepared by SEBA Bank AG ("SEBA") in Switzerland. SEBA is a Swiss bank and securities dealer with its head offce and legal domicile in Switzerland. It is authorized and regulated by the Swiss Financial Market Supervisory Authority (FINMA). This document is for your information only and is not intended as an offer, or a solicitation of an offer, to buy or sell any investment or other specific product.

SEBA is not an authorised person for purposes of the Financial Services and Markets Act (FSMA), and accordingly, any information if deemed a financial promotion is provided only to persons in the UK reasonably believed to be of a kind to whom promotions may be communicated by an unauthorised person pursuant to an exemption under the FSMA (Financial Promotion) Order 2005 (the "FPO"). Such persons include: (a) persons having professional experience in matters relating to investments ("Investment Professionals") and (b) high net worth bodies corporate, partnerships, unincorporated associations, trusts, etc. falling within Article 49 of the FPO ("High Net Worth Businesses"). High Net Worth Businesses include: (i) a corporation which has called-up share capital or net assets of at least GBP 5 million or is a member of a group in which includes a company with called-up share capital or net assets of at least GBP 5 million (but where the corporation has more than 20 shareholders or it is a subsidiary of a company with more than 20 shareholders, the GBP 5 million share capital / net assets requirement is reduced to GBP 500,000); (ii) a partnership or unincorporated association with net assets of at least GBP 5 million and (iii) a trustee of a trust which has had gross assets (i.e. total assets held before deduction of any liabilities) of at least GBP 10 million at any time within the year preceding the promotion. Any financial promotion information is available only to such persons, and persons of any other description in the UK may not rely on the information in it. Most of the protections provided by the UK regulatory system, and compensation under the UK Financial Services Compensation Scheme, will not be available.

SEBA BANK

SEBA Bank AG
Kolinplatz 15 • 6300 Zug • Switzerland • info@seba.swiss • seba.swiss

Crypto.Banking.Simplified.