Report

Zero-Knowledge Proofs in Blockchain Finance: Opportunity vs. Reality

Nethermind & Deutsche Bank

December 2025

NETHERMIND

In partnership with Deutsche Bank

Table of Contents

Letter from the Leadership **4**
Executive Summary **5**
Understanding Zero-Knowledge **8**
The Prover and the Verifier: Roles in the Protocol 8
The Three Properties of a Zero-Knowledge Proof System 9
Illustrative Example: The Ali Baba Cave Analogy 9
Connecting to the Three Properties 10
Blockchain ZKP: Use Case Ideas vs. Reality **13**
Private On-chain Transactions and Asset Management 13
Know-your-Customer and Anti-Money Laundering 15
Proof of Reserves 17
Blockchain Scaling Solutions 19
Blockchain ZKP: Case Studies in the Market **23**
Private On-chain Transactions and Asset Management 23
Know-your-Customer & Anti-money Laundering 24
Proof of Reserves 25
Blockchain Scaling Solutions 26
Blockchain ZKP: Challenges and Trends **30**
Challenges 30
A Convergence of Trends 31
The Way Forward: The Future of ZKPs in Blockchain Finance **34**
From Theory to Practice: Use Cases and Market Examples 34
Why This Matters: The Stakes for Blockchain and Financial Services 35
Appendix: Glossary of Key Terms **37**
References **40**
About us **42**
Authors 42

01

Letter from the Leadership & Executive Summary

Zero-Knowledge Proofs in Blockchain Finance: Opportunity vs. Reality

Letter from the Leadership

The digital assets market stands poised for transformative growth, ready to integrate with traditional financial services. Catalysts such as enhanced service delivery, greater transparency, and round-the-clock operations are accelerating this shift. Yet, trust and privacy remain a critical hurdle. The fallout from "crypto winters" and high-profile blockchain scandals has left businesses questioning how to navigate this evolving landscape. Furthermore, while the permissionless and public nature of the most popular blockchains attracts capital and innovation, it also raises questions about privacy.

Cybersecurity will be central to this evolution—protecting client funds and safeguarding information will help define the winners in this new landscape. Zero-knowledge proofs (ZKP) are designed to ensure that data can be verified as true without revealing any additional information. As new legislation emerges to protect clients and stabilise financial markets, companies face a pivotal moment: build models that meet the demands of this paradigm shift—or risk falling behind.

This paper explores the opportunities, challenges, and real-world applications of ZKP technologies in securing digital assets. We highlight key lessons from companies experimenting with these models—some succeeding, and others revealing where more work is needed. Our aim is to spark deeper awareness and accelerate the development of tools that protect customer data and shape the digital assets models of the future.

Sabih Behzad
Head of Digital Assets and
Currencies Transformation

Deutsche Bank

Daniel Celeda
Chief Executive Officer

Nethermind

D. Celeda

Executive Summary

In this paper, we argue that there is strong potential for the development of ZKP as a method of protecting clients, assets, and transaction data, however more work needs to be done to fully meet some of the challenges that exist including lack of clear regulations, the need for standardisation, high throughput costs in some cases, and human factors that can be difficult to overcome. This paper is primarily focused on the financial sector – banks, markets, payments, and institutions – as it touches all commercial enterprises.

A number of regulations highlight the reality that better security for financial services, and blockchain in particular, is not just a "nice to have". In the EU and United Kingdom, eIDAS[1] (electronic identification, authentication, and trust services) rules "secure cross-border transactions by establishing a framework for digital identity and authentication." In the United States, the GENIUS Act[2] will require stablecoin issuers to meet the requirements under the Bank Secrecy Act, which means strong anti-money laundering requirements. Consequently, to meet these regulatory requirements, counterparties in the banking system will need to adopt privacy-preserving mechanisms that remain compliant while protecting sensitive financial information. More broadly, financial institutions must transition toward scalable and secure system architectures that can support client needs and safely integrate blockchain-based technologies.

In section 3, we start with an overview of some of the core concepts for ZKP to help clarify terminology used in this paper, including the role of the Prover, who would like to prove data, and the Verifier, who needs verification that the data is correct. In sections 4 and 5, we delve into a more detailed explanation for some ZKP use cases and then dive into examples of tests or live implementations in the market. These use cases include:

- **Private On-chain Transactions and Asset Management:** Transactions are privately recorded and validated directly on a blockchain's main network, offering higher security from tampering once confirmed, while digital assets can be used as collateral without revealing the leveraged position. All of that can be done in accordance with existing AML/KYC regulations, like the travel rule, which requires virtual assets service providers (VASPs) to share beneficiary and transaction information for transfers.

- **Know-your-customer (KYC)/Anti-money Laundering (AML) Verification:** These are digital representations of identity attributes used to prove identity. Verifiable credentials are a great enabler of automated KYC and AML control over assets. They can be ported to help prevent onerous and repetitive identity verification processes.

- **Proof of Reserves (PoR):** This is a process that verifies a crypto exchange holds enough assets to cover all user deposits. This supports operational and liquidity models for a functioning system of payments and transactions. It can also be used as verification for other products, such as collateral lending, where the assets must be confirmed to lend against.

- **Blockchain Scaling Solutions:** This enables a computer to offload the computation of some functions while maintaining verifiable results. Such solutions are designed to reduce costs and increase efficiency.

The examples that support these use cases encompass a diverse range of actors. These include crypto exchanges that are implementing zk-SNARKs[3], i.e., a proof construction where one can prove possession of certain information; a public-private partnership between the Bank of England and MIT to test private retail CBDC transactions[4]; and a proof of concept between Deutsche Bank and Privado ID to test the interplay between ZKP, digital identity and KYC[5]. These organisations span geographies and products, but they are all testing ZKP to understand how it works and the potential limitations for success.

In the last couple of sections, we reiterate some of the challenges and issue a call to action for businesses, banks, regulators, trade associations, tech companies, and cybersecurity teams to continue to test models that can help improve services more broadly. The issue of privacy is one that will be solved through rigorous experimentation and data sharing about how models perform in different settings. Change is coming to the financial services market, and traditional models will need to develop in a direction that aligns with the digital asset's models of the future.

02

Understanding Zero-Knowledge

Zero-Knowledge Proofs in Blockchain Finance: Opportunity vs. Reality

Understanding Zero-Knowledge

The modern concept of zero-knowledge proofs originates from the 1985 paper "The Knowledge Complexity of Interactive Proof Systems" by Goldwasser, Micali, and Rackoff[6], which introduced the idea that a Prover can convince a Verifier of a statement's validity without revealing any additional information. This foundational work defined the security properties and interaction model that underpin all ZKP systems today.

In the early 2010s, the field evolved from theoretical constructs to practical cryptographic tools. ZK-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) introduced proofs that are extremely small and fast to verify, enabling applications where both scalability and privacy are essential. Following, zk-STARKs (Zero-Knowledge Scalable Transparent ARguments of Knowledge)[7] emerged as a transparent alternative, removing the need for trusted setups and offering provable post-quantum security through the use of hash-based cryptography and probabilistically checkable proofs. Together, these advances transformed ZKPs from academic concepts into building blocks for real-world, large-scale systems.

In parallel, in 2008, blockchains, as we know them today, commenced following the publication of the whitepaper "Bitcoin: A Peer-to-Peer Electronic Cash System" by author (or authors) Satoshi Nakamoto[8]. This was followed by Ethereum's whitepaper authored by Vitalik Buterin in 2015. Since these early developments, the development of ZKP has grown and there are more market-ready use cases.

To appreciate the strategic value of zero-knowledge proofs, it is first necessary to understand their fundamental components and the guarantees they provide. This section demystifies the core concepts of ZKP systems, using clear definitions and intuitive analogies to build a solid foundation for the business applications that follow.

The Prover and the Verifier: Roles in the Protocol

Every ZKP interaction involves a cast of well-defined participants and a crucial piece of information.

The Prover

This is the entity that aims to prove a claim is true. The Prover possesses a piece of secret information, called "the witness", that substantiates the claim and uses it to generate a cryptographic proof. In a financial context, the Prover could be a customer proving they meet the criteria for a loan, a fund manager proving their portfolio adheres to risk limits, or a bank proving it holds sufficient reserves. For example, a Prover that holds $12,000 worth of assets could use that information to show that the claim "I hold more than $10,000" is true. The actual value of the assets, $12,000, is the witness.

When implementing ZKPs with blockchains, the proof generation algorithm is usually run off-chain. This happens for two reasons. First, the proof computation is computationally demanding and could be very expensive to be performed on-chain due to the high on-chain computation cost. Second, on-chain computation would reveal the aforementioned secret piece of information i.e., the witness.

The Verifier

This is the entity that needs to be convinced of the claim's truth but should not learn the secret information. The Verifier receives the proof from the Prover and runs a verification algorithm to check its validity. The Verifier could be a lending institution, a regulator, an auditor, or the general public. When ZKPs are deployed in a blockchain scenario, the verification algorithm is usually implemented as an on-chain smart contract, which allows the public to ensure that the verification algorithm works properly and doesn’t accept invalid proofs.

The Three Properties of a Zero-Knowledge Proof System

For a ZKP system to be both trustworthy and useful, it must satisfy a set of core properties. These properties are not just technical features; they are the foundation of the business guarantees that ZKPs provide.

1. **Completeness: The Guarantee of Functionality**. If a statement is genuinely true, an honest Prover can always convince an honest Verifier of this fact.
2. **Soundness: The Guarantee Against Deception**. If a statement is false, a dishonest Prover cannot trick an honest Verifier into believing it is true, except with a probability so small it is considered negligible. (We note that for ZKP deployment “negligible” refers to events that happen with probability 2^{-80} or less, which is a one in septillion chance).
3. **Zero-Knowledge: The Guarantee of Privacy**. The zero-knowledge property guarantees that if a statement is true, the Verifier learns absolutely nothing beyond the fact that the statement is true. The proof itself leaks no information about the secret witness used to generate it.

Illustrative Example: The Ali Baba Cave Analogy

The most famous analogy used to explain the core properties of a ZKP is the story of Ali Baba's cave[9], which involves a Prover (Peggy) and a Verifier (Victor).

The Setup: Imagine a ring-shaped cave with a single entrance that splits into two paths, Path A and Path B. These paths are connected at the back by a locked door that can only be opened with a secret password. Peggy claims she knows the password, and Victor wants to buy it from her, but first, he needs proof that she actually knows it. Peggy, however, doesn't want to reveal the password itself, as Victor could then use it without paying.

The Protocol: To prove her knowledge, they agree on the following interactive protocol:

- Peggy enters the cave alone and walks down one of the paths (e.g., Path A), hidden from Victor's view.
- Victor then walks to the entrance and randomly shouts the name of a path he wants Peggy to emerge from (e.g., "Come out of Path B!").
- **If Peggy knows the password**, she can open the magic door at the back and switch paths if necessary. She will always be able to emerge from the path Victor called out.
- **If Peggy does not know the password**, she is stuck on her original path. She can only emerge from the correct path if Victor, by pure chance, happens to call out the path she initially chose. She has a 50% chance of getting lucky.

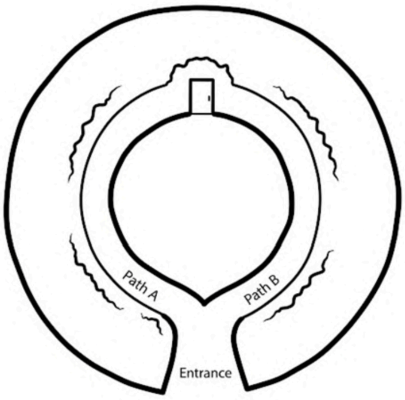

Illustration 1: Peggy must emerge from the correct path to for Victor

Connecting to the Three Properties

This simple story demonstrates the core principles of an interactive ZKP:

- **Completeness:** If Peggy truly knows the password (the statement is true), she will successfully complete the challenge every single time, convincing Victor.
- **Soundness:** A single successful attempt is not convincing, as Peggy could have been lucky. However, if they repeat the protocol 80 times, the odds of Peggy guessing correctly every time are one in 2^{80}. After enough successful rounds, Victor can be statistically certain that Peggy is telling the truth. The soundness of her claim is established with overwhelmingly high probability.
- **Zero-Knowledge:** Throughout this entire process, Victor becomes convinced that Peggy knows the password, but he never sees or hears the password itself. He gains zero knowledge about the witness.

While illustrative, modern ZKPs, especially those used in blockchain, are often non-interactive, which we will explore next.

Non-interactive ZKP

Taking the Ali Baba cave example further, one could consider what would happen if this interaction were recorded so that the data could be verified later or without authorisation. Even if a third party, like a judge, watches a video of 80 successful trials, the video is worthless as proof for an ensuing case. The judge cannot know whether Victor and Peggy colluded ahead of time on the sequence of challenges, which would allow a dishonest version of Peggy to succeed every time. This illustrates a key limitation of interactive proofs: they are not transferable. For applications like public blockchains, where any independent party must be able to verify a proof at any time, non-interactive ZKPs are required. Fortunately, most modern interactive proof systems can be made non-interactive relatively easily by applying the so-called Fiat—Shamir transformation[10]. The Fiat-Shamir transformation essentially allows Victor's random challenge to be generated deterministically, by using hash-functions in a way that he can later verify wasn't rigged, thus removing the need for interaction. In the non-interactive proof systems, Prover's proof is a single piece of data handed to the Verifier. That is, no communication with the Verifier is required before the proof is completed.

Succinctness

Succinctness means that the proof size is short compared to the length of the statement it proves (e.g., in the case of verifiable computation, the proof is short compared to the size of computation that is being proved). Shorter proofs usually come with a shorter time needed for the Verifier to check the proof. This is especially important for blockchain applications of ZKP. The distributed nature of modern blockchains, where each of the nodes re-execute all the network's operations, puts a limit on the amount of computation such networks can perform. This also applies to the verifiability of ZKPs. For ZKP to be usable in blockchains, they need to have both short proofs (as blockchain storage is expensive) and efficient verification (as blockchain compute is limited). This translates to lower transaction fees and efficiency gains.

03

Blockchain ZKP: Use Case Ideas vs. Reality

Zero-Knowledge Proofs in Blockchain Finance: Opportunity vs. Reality

Blockchain ZKP: Use Case Ideas vs. Reality

Having established the foundational principles and guarantees of ZKPs, this paper now explores their impact within the financial services industry. ZKPs are not a solution in search of a problem; they offer direct and powerful answers to some of the most pressing challenges in modern finance, from scalability and trust to privacy and compliance. However, it is important to temper this potential with the understanding that ZKPs are not a panacea. Models still need to consider non-ZKP privacy issues, such as human error, implementation bugs, and cybersecurity attack vectors, which could also have an impact on security.

It is also important to highlight the impact that ZKP can have when we consider the use of public vs. private blockchains. Many financial institutions are still developing their understanding of how to share data across different types of blockchains and with different organisations and companies. Global financial systems depend on interoperability, a principle equally vital for blockchain's adoption.

In this section, we examine how ZKPs can support secure, privacy-preserving interoperability between public and private blockchains. It will cover four opportunities as well as some of the challenges being faced by each topical area. This is meant to showcase the ways that companies and organisations can consider opportunities for their organisation while also identifying critical areas for continued development. The topics covered include (1) privacy preserving transactions and asset management, (2) Know-your-Customer and Anti-Money Laundering, (3) proof of reserves and (4) blockchain scaling solutions. While not exhaustive, these four areas represent intersections of ZKP capabilities with pressing financial services priorities.

Private On-chain Transactions and Asset Management

The Business Problem

The inherent transparency of public blockchain is a double-edged sword, since it makes them unsuitable for some real-world financial activity. Institutions cannot broadcast their trading strategies, client positions, or transaction flows on a public ledger for all competitors to see. On the other hand, early privacy-centric cryptocurrencies, which offer strong anonymity, have faced intense regulatory scrutiny due to concerns that they could be used to facilitate illicit finance. The central challenge is achieving transactional privacy while simultaneously demonstrating regulatory compliance.

The ZKP Solution: Compliance by Design.

ZKPs offer a unique solution that reconciles these opposing requirements by enabling privacy that is conditional and auditable.

- **Shielded Transactions:** The basic mechanism, pioneered by cryptocurrencies like Zcash, uses ZKPs, specifically zk-SNARKs to create "shielded transactions." In these systems, transaction details like the sender, receiver, and the amount are represented not as visible account balances but as private notes (i.e., cryptographic commitments to the original transaction data). When a user spends funds, they consume one or more existing notes and produce new ones, but all details remain encrypted. What is broadcast to the blockchain is a so-called "nullifier" (a value that prevents double-spending of private notes) and a ZKP that proves the validity of the transaction (i.e., the sender had sufficient funds to send, and no money was created or destroyed in the transaction) without revealing any of the confidential details.
- **Embedding Compliance Rules in the Circuit:** The key innovation for institutional finance is to extend this concept by embedding regulatory rules directly into the ZKP's "circuit". A ZKP for a financial transaction could be constructed to prove not only that the transaction is valid, but also that it adheres to a specific set of compliance rules. The proof could cryptographically verify statements such as:
    - "The value of this transaction is below the €10,000 AML reporting threshold." This is achieved using a "range proof" i.e., a specialised ZKP that proves a secret number lies within a public range
    - "Neither the sender's nor the receiver's identity is associated with an address on the OFAC sanctions list". This is done by using a non-membership proof, a ZKP that shows that values (here the senders and receiver's identities) don't belong to a particular set (here the OFAC list).
    - "Both the sender and receiver possess a valid KYC credential from a trusted issuer". This is done by a combination of membership proofs and a ZKP for the issuer's signature verification.
- **Selective De-anonymization:** To address the need for lawful access, these systems can be designed with a "viewing key" or a "compliance key." The transaction data can be encrypted so that it remains private to the public but can be selectively decrypted by a designated, authorized party (such as a regulator or internal compliance officer) under specific, legally sanctioned conditions. This creates a system that is private by default but auditable when required, balancing confidentiality with accountability.

Potential Benefits for the Financial Sector

- **Confidentiality:** Enables institutions to leverage the unique benefits of blockchain technology (e.g., immutability, atomic settlement, global access) without exposing sensitive client data or proprietary trading strategies. This confidentiality can also be extended to the private use of digital assets. For example, ZKPs could theoretically allow the utilization of digital assets as collateral without revealing the asset owner's position or leverage.
- **Proactive, automated compliance:** This model shifts compliance from a reactive, after-the-fact auditing process to a proactive, automated one that is cryptographically

enforced at the protocol level. This has the potential to dramatically reduce the cost and complexity of compliance programs.

- **GDPR compliance on public blockchains.** . A fundamental challenge that comes with the use of public blockchains by financial institutions relates to the immutable and transparent disclosure of clients' Personally Identifiable Information (PII) on a public ledger, which is an important concern for transactions or even simply holding customer data. The European Data Protection Board (EDPB)[11] recommends that personal data should not be processed on the blockchain itself and advises using off-chain storage with on-chain hashes instead. ZKPs could then utilize these hashes to prove a statement is correct.

Implementation Challenges

- **Legal ambiguity of ZKP-based evidence:** Given the number of jurisdictions a global bank must cover, there are reasons to be concerned about data and privacy standards. Companies must carefully assess the rules and guardrails they must adhere to in each transaction. Mistakes, especially as they relate to data protection, can be costly.
- **Complexity of translating compliance policies to circuits:** Compliance policies are often complex and ambiguous, which makes them difficult to translate into logical circuits.

Know-your-Customer and Anti-Money Laundering

The Business Problem

For any financial institution, Know-your-Customer and Anti-Money laundering compliance is a legal mandate and a significant operational burden. The current process is cumbersome, repetitive for the customer, and expensive for institutions. Each time a customer onboards with a new service, they are repeatedly required to submit sensitive identity documents, such as passports and utility bills. The institution must then verify these documents and store them securely, creating a set of PII that is a prime target for cyberattacks and a major source of regulatory liability under frameworks like EU General Data Protection Regulation (GDPR)[12].

The ZKP Solution: Self-Sovereign Identity with Verifiable Credentials

ZKPs are a core component of an emerging digital identity model known as Self-Sovereign Identity (SSI), which gives individuals control over their own data. The system involves three roles: an Issuer, a Holder, and a Verifier.

How it Works:

- An **Issuer** (e.g., a government, university, or bank) issues a digitally signed, tamper-proof credential to a user. This is the Verifiable Credential (VC). For example, a government could issue a digital passport VC.
- The **Holder** (the user) stores this VC securely in a private digital wallet on their phone or computer. The data lives with the user, not in a centralized database.
- A **Verifier** (e.g., a new financial service the user wants to access) requests proof of a specific attribute from the user and verifies its correctness. Part of it could be checking a list of revoked credentials kept by the Issuer.

The ZKP Benefits – Selective Disclosure & Predicates

Here, ZKPs could enable a key shift. Instead of sharing the entire VC, the Holder uses their wallet to generate a ZKP about a claim related to the data within the VC. This is known as "selective disclosure".

- **Example 1: Age Verification**. A user can generate a ZKP that proves the statement "the date of birth in my government-issued VC is more than 18 years ago" without ever revealing their actual birthdate.
- **Example 2: Reusable KYC**. In theory, a customer who has completed a full KYC process with Bank A can be issued a "KYC-Verified" VC. When they want to open an account at Bank B, instead of starting the process from scratch, they could simply present a ZKP derived from their VC. This proof would cryptographically attest that "this user holds a valid, non-revoked credential from a trusted issuer that confirms they have passed KYC checks." Bank B can verify this proof instantly without ever seeing the original documents or even knowing that Bank A was the original verifier.

Potential Benefits for the Financial Sector

- **Reduced Onboarding Friction & Cost:** KYC checks become instantaneous and reusable, transforming a days-long process into a seconds-long one. This dramatically improves the customer experience and slashes the operational costs associated with manual verification.
- **Minimized Data Liability:** The institution verifies the necessary facts (e.g., "user is over 18 years old") without ever possessing or storing the underlying PII. This could reduce the scope of compliance and mitigate the financial and reputational risk of data breaches. This is especially important for blockchain applications. Since blockchains are immutable, they should not store any PII data, as such storage is permanent.
- **Interoperability and Ecosystems:** A VC issued for banking can be reused for on-chain insurance, various decentralised exchanges, or other services, creating a seamless and portable digital identity that benefits both consumers and businesses across an entire economic ecosystem.
- **Reusable Regulatory Profiling (Suitability Tests):** Customers can complete suitability and risk-profiling assessments once and reuse the resulting attestations across banks and investment platforms. ZKPs allow trusted issuers to release a VC for eligibility

("high-risk tolerance", "professional investor") without sharing sensitive details, reducing repetitive compliance work.

Implementation Challenges

- **Requires Ecosystem Buy-In and Standards:** Some opportunities, such as onboarding, struggle due to the lack of consistent policies and data formatting. Without agreement on how data is shared and alignment on standardised systems, these efforts are unlikely to see full benefits. There is also the challenge of inter-institutional trust, which would be needed to support this effort.
- **Initial Infrastructure Setup Cost:** Ensuring policies have aligned design standards is likely to be costly. This could leave some scope for a consortia or regulators to help support infrastructure development.
- **Technology Maturity.** Until recently, it was almost infeasible to compute ZKPs on mobile devices or home computers, which severely limited the usefulness of verifiable credentials. However, with the advancements on both the theoretical side and engineering, it is becoming more feasible for them to derive ZKPs. However, current development tools are generally not designed for personal devices.
- **ZKP Evidence:** The evidentiary standards for ZKP-based proofs remain a critical consideration. Different banks and regulators will retain diverse requirements for data collection, retention, and the precise standard of what constitutes valid proof. Further to this, organisations will need to carefully assess provenance and reliability of the underlying data. For example, a driver's license might be good enough in one location, but not enough for a regulator in another jurisdiction or bank.

Proof of Reserves

The Business Problem

The digital asset industry has been plagued by high-profile collapses of centralized exchanges and custodians (e.g., FTX, Celsius), largely driven by the mismanagement and commingling of customer funds. This has created intense regulatory and market pressure for any institution holding customer assets to prove its solvency, that is, to demonstrate that it holds sufficient reserves to cover all customer liabilities. This issue highlights a key difference: traditional regulated exchanges hold clients' assets in segregated trust accounts, which prevents pooling. In contrast, many digital asset exchanges custody the assets themselves and may even use them in financial instruments. Traditional financial audits are slow, costly, and only provide a point-in-time snapshot. Early attempts at on-chain Proof of Reserves were flawed[13], as they often leaked sensitive commercial information (like an exchange's total assets under management) or could be easily manipulated.

The ZKP Solution: Cryptographic Proof of Solvency

ZKPs enable a robust, privacy-preserving, and continuously verifiable Proof of Reserves system. A state-of-the-art implementation involves several cryptographic steps:

- **Proof of Assets:** The institution generates a ZKP to prove that it controls the private keys corresponding to a specific set of on-chain assets, thereby proving its ownership of those reserves.
- **Proof of Liabilities:** The institution aggregates all its customer liabilities into a cryptographic data structure, e.g., a Merkle tree. The root hash of this tree acts as a succinct and binding commitment to the total sum of liabilities. Crucially, each individual customer can be given the data needed to independently and privately verify that their specific account balance is correctly included in the tree, without them seeing any other customer's data. This prevents the institution from selectively omitting liabilities.
- **The Solvency Proof:** The institution then generates a final ZKP. This proof attests that the total value of the assets proven in the proof of assets is greater than or equal to the total value of the liabilities proven in the proof of liabilities.
- **Anonymity and Privacy:** The proof of assets can be constructed to prove the total value of reserves without revealing the specific blockchain addresses or the exact total amount, protecting the institution's sensitive financial position from competitors. Similarly, the proof of liabilities protects the privacy of all customers.
- **Preventing Manipulation with Range Proofs:** A critical component of the solvency proof is the use of a ZKP range proof on each customer liability. This proves that every individual liability included in the Merkle tree is non-negative. This prevents a common attack where a fraudulent institution could create a fake account with a large negative balance to artificially reduce its total stated liabilities and appear solvent.

Potential Benefits for the Financial Sector

- **Enhanced Trust and Transparency:** This system provides near-real-time, cryptographic assurance of solvency that can be verified by customers, auditors, and regulators. It moves the industry from a "trust me" model based on periodic, opaque reports to a "verify me" model based on continuous, mathematical proof.
- **Reduced External Audit Costs:** By automating a significant portion of the asset and liability verification process, ZKP-based PoR could streamline audits, reducing the reliance on and costs associated with traditional third-party auditors.
- **Competitive Differentiation:** In the wake of industry crises, the ability to provide a strong, privacy-preserving Proof of Reserves is a powerful competitive differentiator that could help attract and retain customer assets.

Implementation Challenges

- **Does not prevent all forms of fraud (e.g., asset theft):** A proof only attests to the assets controlled at the time of proof generation. Exchanges could temporarily move assets to pass PoR monitoring.
- **Not an agreed audit method:** Regulatory authorities (including central banks, securities regulators, prudential supervisors) and audit and standards organisation have not formally endorsed PoR as a standard auditing method. Most organisations are focused on PoR as a transparency tool that can align with traditional methods of auditing.

Blockchain Scaling Solutions

The Business Problem

With financial institutions becoming more interested in utilizing public blockchains, there is a need to address two conflicting requirements: (1) maintaining the public nature of the blockchain, which ensures it can serve as a common backbone that connects otherwise siloed infrastructures of the participating parties; and (2) ensuring that with the growth of the information processed on blockchains, its performance is not impeded. The latter is particularly difficult to achieve as the current design of the most popular blockchains require all nodes in the network to re-execute the entire network's computation, e.g., smart-contract transactions and transfers.

The ZKP Solution: Execute Once, Verify Everywhere

Verifiable computation using ZKPs flips this model on its head, enabling a paradigm of "execute once, verify everywhere". The core idea is to separate the computationally heavy work of execution from the lightweight work of verification.

- **The Big Server vs. Small Client Model:** In this scenario, a powerful, untrusted server (the Prover) is tasked with a complex computation, such as running a Monte Carlo simulation for risk assessment. After completing the task, the server uses the inputs and outputs to generate a small, succinct ZKP that attests to the correctness of the execution. The financial institution (the Verifier) can then receive the result and the proof. Verifying this proof is computationally trivial, requiring a fraction of the resources needed for the original calculation. This establishes a trustless and cryptographically auditable relationship with any computational provider, be it a cloud service or a data analytics partner. In decentralised finance (DeFi) applications that depend on computationally demanding tasks, like simulations and risk parameter calculations, ZKPs are used to outsource heavy computation from the blockchain to a computationally cheaper environment. In that scenario, a DeFi smart contract doesn't perform the computation itself, but only verifies the computation provided by an external service.

- **Outsourcing Blockchain Computation (zk-Rollups):** This is arguably the most impactful application of verifiable computation in the blockchain space today, directly addressing the blockchain scalability problem. Instead of processing every transaction on the expensive Layer 1, e.g., Ethereum, a zk-rollup bundle executes thousands of transactions in a low-cost environment such as a Layer 2. The rollup then generates a single, succinct ZKP that proves the validity of the entire batch of transactions. This one small proof is then posted to the main blockchain, where it is quickly and cheaply verified by an on-chain smart contract. This allows the main chain to securely validate thousands of transactions by verifying just one proof, without having to re-execute all of them.

Potential Benefits for the Financial Sector

- **Reduced Costs:** For DeFi applications and other on-chain activities, zk-rollups can lower transaction costs by 90-99%, making services like stablecoin payments, frequent trading, and complex smart contract interactions economically feasible.
- **Increased Scalability:** By moving execution off-chain, zk-rollups can increase the transaction throughput of a blockchain from a few dozen transactions per second (TPS) to several thousand TPS. While a significant leap for public blockchains, TPS still requires further advancements to truly match peak throughput demands of global financial markets.
- **Inherited Security:** Unlike some other scaling solutions that rely on economic incentives and fraud detection windows, zk-rollups inherit the security and finality of the underlying blockchain. The validity of every state transition is guaranteed by cryptographic proof, not just by the assumption that a malicious actor will be caught.
- **New DeFi Possibilities:** The combination of scalability, low cost, and privacy unlocks a new design space for more sophisticated on-chain financial products. This includes privacy-preserving derivatives markets, undercollateralized lending protocols based on private credit scoring, and efficient, complex arbitrage strategies that were previously impossible on-chain.

Implementation Challenges

- **High Prover-side Computational Overhead:** Adoption levels are currently being hindered by the relative costs related to the computational resources needed to generate proofs. For example, in the case of zk-rollups, proving a rollup's state transition is usually 2000x - 5000x more computationally expensive than just re-executing the transition.
- **Complexity of Circuit Development:** Developers utilise various domain-specific languages (DSLs) like Cairo, Circom, Noir to reduce the engineering overhead that comes with making the program execution provable. These languages require developers to obtain a new skillset and ensure a high level of attention to detail, as an incorrectly implemented program might not provide the required functionality and security.

Table 1: Summary of ZKP Use Cases in Finance

Use Case	Business Problem Solved	ZKP Solution	Primary Benefits	Key Implementation Hurdles
Private On-chain Transactions and Asset Management	Lack of confidentiality on public ledgers Regulatory risk of privacy coins	Shielded transactions with compliance rules embedded in the ZK circuit	On-chain confidentiality Automated compliance Automated regulatory adherence	Legal ambiguity of ZKP-based evidence Complexity of designing compliant circuits
Know-your-Customer and Anti-money Laundering	Inefficient/costly KYC Poor customer experience High data security liability	Self-Sovereign Identity (SSI) with ZK-powered Verifiable Credentials (VCs)	Reduced data liability (GDPR) Instant, automated, reusable KYC Enhanced fraud prevention	Requires ecosystem buy-in/standards Initial infrastructure setup cost Technology maturity Lack of legal recognition of ZKPs as valid proofs Cross-bank, cross-jurisdictional KYC/AML requirement variation
Proof of Reserves	Lack of verifiable solvency for custodians Slow, point-in-time audits	Cryptographic proof of assets vs. liabilities using Merkle trees and range proofs	Enhanced customer/ regulator trust Reduced external audit costs Continuous, verifiable proof of solvency Preserves institutional & client privacy	Does not prevent all forms of fraud (e.g., asset theft) Not an agreed audit method
Blockchain Scaling Solutions	High cost/risk of outsourcing computation Blockchain scalability limits	ZK-rollups Off-chain proving of complex calculations	Reduced operational/ transaction costs Scalability Rollup security Trustless third-party computation	High prover-side computational overhead Complexity of circuit development

04

Blockchain ZKP: Case Studies in the Market

Zero-Knowledge Proofs in Blockchain Finance: Opportunity vs. Reality

Blockchain ZKP: Case Studies in the Market

Zero-knowledge proofs help ensure that data is secure and meets the right product-market fit for development. Over the last several years, many new use cases have come to the fore, and there are opportunities to learn from the examples supplied by other organisations. Building on the conceptual framework of ZKP use cases (section 3), this section delves into specific market examples, highlighting practical implementations in the industry. While this is not an exhaustive list, it provides concrete examples of ZKP implementation within the financial services sector.

Private On-chain Transactions and Asset Management

With fewer stores accepting cash payments and concerns about monetary policy implications, there has been increased discussion regarding retail central bank digital currency (e.g., digital pound or digital euro). While physical cash offers a high degree of anonymity, its utility is limited in an increasingly digital economy, conversely most electronic payment systems inherently create traceable records, raising privacy concerns. For example, a company that records the transaction could face a cyber-attack and its transactions could become known or monitored. Some countries, such as the United States, have specifically stopped development of and banned the use of retail CBDCs[14] and concerns have been raised in the UK and China about a government's potential ability to track citizens' spending. The tracing aspect can lead to low uptake at a time when governments are considering their central bank's role in the financial system, competition, and financial inclusion.

To preserve public acceptability of CBDCs, there are efforts designed to offer cash-like privacy with compliance, so a retail CBDC can launch without becoming a surveillance rail. ZKP gives a path to minimize who sees what, when they can see data, and reduces data liability for intermediaries and the central bank while still enabling targeted law-enforcement access. ZKP identity helps reduce some aspects of KYC/AML friction and data-handling risk via data minimisation by design, enabling reuse of bank-issued credentials across products and partners. It is important to remember that CBDCs are just one example of how private and compliant transactions will play a role in the work being done to support blockchain payments. Other blockchain transactions are likely to need this technology as well.

Example 1: Bank of England/MIT Digital Pound

In 2024, the Bank of England and the Massachusetts Institute of Technology Digital Currency Initiative published a paper[4] regarding privacy of the digital pound. The development of CBDC faces major hurdles over concerns that government entities could see how individuals are spending their digital cash, when this is meant to be for personal, private use. It is important to note that this was a design and feasibility study rather than a product implementation, but it documents concrete ZK-backed patterns for selective disclosure in CBDC payments.

The goal of the project was to design a space where a hypothetical digital pound gives strong user privacy by default while meeting AML/Countering the Financing of Terror (CFT) obligations. The design centred on evaluating PETs (including ZK) that the BoE could adopt in its platform architecture. The paper analyses how ZK proofs, pseudonymization, and secure multiparty computation can support attribute-level attestations (e.g., "KYC-passed," "below threshold") so the core system, and even the central bank, can operate without access to raw PII.

Example 2: BIS Project Tourbillon

In 2023, the Bank for International Settlements (BIS) Innovation Hub Swiss Centre launched "Project Tourbillon"[15], which focused on payer anonymity. The goal of this effort was to test whether a retail-CBDC could deliver cash-like payer anonymity while remaining secure and scalable, i.e., whether a central bank can see aggregates and risks without touching personal data. In this experiment, there was a focus on merchant transaction tracking only with the central bank unable to see activity of customers or merchants.

Tourbillon prototyped two e-cash style designs focused on meeting three key goals of (1) privacy through the enablement of payer anonymity, (2) security by implementing quantum-safe cryptography; and (3) scalability by testing the prototype's ability to handle a growing number of transactions using payment data. BIS tested two different options called eCash 1.0 and eCash 2.0, which were similar but differentiated by how the central bank in each project would track CBDC spend. The first test, eCash 1.0, focused on redemption and tracking of spent CBDC, while eCash 2.0 focused on the unspent CBDC.

There were three key findings of this effort, including that (1) it is feasible to build a prototype, but this needs to be tried at scale, (2) this can be done at high speed with thousands of transactions per second, and (3) quantum-safe technology can be implemented for future security. While they noted that these options are possible, it is not without challenges, especially when it came to the quantum-safe cryptography, which "exhibited slow performance and limited functionality, with throughput." They also highlighted that, "a comparison of the two prototypes illustrates the trade-offs between privacy and security: EC1 provides unconditional payer anonymity but EC2 has more resilient security features allowing for better protection against counterfeiting." It is clear that more work will need to be done to support market-ready developments.

Know-your-Customer & Anti-money Laundering

Ensuring that your clients are who they say is an important step towards ensuring that your business protects itself and other customers. The United Nations Office on Drugs and Crime has estimated that anywhere between €715bn and €1.87tn[16] is laundered each year. Companies have a responsibility to take steps that prevent fraud and other forms of criminal activity. Blockchain digital IDs, ZKP libraries, and allowlists and blocklists are some of the tools that can help support these goals.

Example 3: Deutsche Bank and Privado ID KYC Proof-of-Concept

In 2024, Deutsche Bank and Privado ID (a rebranding of PolygonID) embarked on a proof-of-concept to securely and transparently verify identities on a blockchain network[5]. As a part of this effort, a live prototype was developed that tied into some of Privado IDs digital ID product offering and credentials could be issued using a QR code. There were three distinct use cases trialled during the programme, which included using digital IDs for: (1) traditional onboarding and ongoing KYC processes, (2) enabling compliant and efficient investment processes, and (3) institutional DeFi liquidity pool access.

While the tests of the digital ID technology were successful, there were some lessons learned. For the investment processes, it was noted that contract design could be enhanced to better support call functions with multiple arguments. The test concerning institutional DeFi liquidity pool access highlighted that while ZKP can streamline the verification of attributes, the underlying requirement for counterparties to possess "sufficient reputation in the market" and to undergo "detailed and costly KYC processes" remains paramount. This highlights that ZKP-based solutions must integrate seamlessly with and enhance, rather than entirely replace, established due diligence frameworks.

Example 4: Google /Sparkasse Wallet Age Verification (Transaction Monitoring/Fraud)

In July 2025, Google open sourced their ZKP libraries following a project in partnership with German Sparkasse banks[17]. They shared that this was being done to support EU age assurance ahead of the EU's eIDAS Regulation[1], which comes into effect in 2026, as well as a hope that developers will integrate this tool as part of efforts related to the growth of the EU Digital Identity Wallet model. The goal of this project was to give relying parties (e.g., a bank) a way to verify a specific attribute—e.g., "is over 18," "holds a valid ID"—without ever handling the user's underlying PII, cutting data liability and fraud risk while meeting fast-growing age-assurance mandates. In April 2025, Google announced it was integrating ZKPs into Google Wallet for "fast and private age verification," with early ecosystem partners (e.g., Bumble app) and more use cases in flight.

Proof of Reserves

In financial services, it is important to understand the level of assets your counterparty must have on hand as a way of meeting its obligation to you. PoR ensures a credible, user-verifiable claim of solvency (at least on the liabilities side) to retain deposits and reduce run risk, without leaking customer data. Over time, a regular PoR cadence builds habit-trust with users and regulators to showcase an institution's ability to safely meet its obligations in the market. Many in the digital assets and regulatory technology (regtech) marketplace have called for stronger models around PoR and highlighted the benefits it could bring to improving trust and accuracy of transactions.

Example 5: Binance and OKX Proof of Reserves

After the 2022 trust shock caused by the FTX collapse, Binance, one of the biggest crypto exchanges, set up a project to let users verify that customer liabilities are fully backed without exposing individual balances[3]. The design relied on ZKPs and improved over a previous PoR solution that relied on Merkle trees that leaked private information and were not robust against malicious users. Similar functionality has been built by another major crypto exchange, OKX. By January 2025, OKX had published its 27th consecutive PoR[18] with over 100% reserve ratios on major assets and they shared that they plan to publish their PoR on a monthly basis.

Blockchain Scaling Solutions

We previously discussed the potential for zk-rollups and the opportunities these could provide for companies in terms of speed, scalability and lower costs. This has been highlighted as the next opportunity to ensure that ZKP and blockchain functionality can be integrated in a way that is more efficient for business needs.

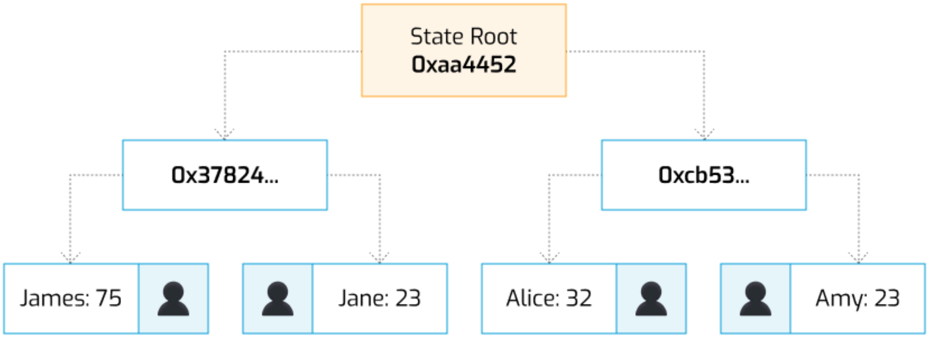

Illustration 2: Model of how a zk-rollup works in practice.

Example 6: Intmax2

In 2023, INTMAX[19] collaborated with Nethermind, and the University of Porto, to formally verify the INTMAX2. INTMAX is a tech company that is working on solutions for privacy-first, "stateless" rollup focused on payments. Nethermind engaged with the team at INTMAX to formalise the key security properties of the INTMAX protocol in the Lean proof assistant. The complexity of the protocol was such that it would not be within the reach of industry standard verification methods and required Nethermind to use significant fragments of Mathlib, the largest computer checkable formalisation of mathematics in existence, e.g., lattice-ordered groups. Over the span of two months, the team formalised in Lean a proof of the financial security properties of the protocol, verifying that the protocol must always hold sufficient funds to fulfil its debts. INTMAX2 relies on trusted aggregators to share the account state. In essence, instead of publishing transactions or account state on-chain, INTMAX posts only compact commitments while users keep and prove their balances locally. This rollup design minimizes on-chain data and trusted coordination but suffers from a more complicated smart contract development process. However, it results in a theoretical transaction throughput of 64000+ transactions/s, on par with the Visa network.

Example 7: Aztec

Aztec[20] is a decentralised privacy-preserving zk-rollup on Ethereum designed to support confidential smart contracts and shielded transactions. Rather than publishing raw transaction data on-chain, Aztec uses ZKPs to commit only to encrypted state transitions while keeping sensitive information such as account balances, transfer amounts, and contract state private to users. Nethermind has been contributing to the Aztec protocol since before mainnet launch, providing engineering support to optimise core components of the early architecture and offering research-driven guidance on improving Layer 2 protocol mechanics. This collaboration has also included work on future decentralisation pathways for Aztec's consensus layer.

Aztec's architecture is built around a note-based model, where value is represented as encrypted commitments, and each spend generates a corresponding nullifier to prevent double-spending. Users interact with contracts through the Aztec client, which compiles private function calls locally and compute ZKPs that attest to the correctness of state updates without revealing underlying data. A Merkle tree of encrypted notes and nullifiers is then updated and published to Ethereum Layer 1 together with the associated validity proofs. This design enables programmable privacy on top of Ethereum, allowing developers to build applications such as shielded transfers, private DeFi interactions, and confidential business logic. Aztec's approach demonstrates how zk-rollups can combine on-chain integrity with strong privacy guarantees suitable for institutional use cases, and Nethermind continues to contribute to the Aztec Network through ongoing research and engineering support on continuous improvement in performance, decentralisation, consensus-layer design and more.

Table 2: Market Examples of ZKP Use Cases

Use Case	Centralised PoR	Privacy Pilots	ZK Identity Solutions
Private On-chain Transactions and Asset Management		Bank of England and MIT DCI "Enhancing the Privacy of a Digital Pound" BIS "Tourbillon" Project	
Know-your-Client / Anti-Money Laundering Verification			DB Privado ID Google/ Sparkassen -Finanzgruppe Bank Account age verification
Proof of Reserves	Binance zk-SNARK deployment OKX zk-STARK deployment		
Blockchain Scaling Solutions		Intamax2 Aztec	

05

Blockchain ZKP: Challenges & Trends

Zero-Knowledge Proofs in Blockchain Finance: Opportunity vs. Reality

Blockchain ZKP: Challenges and Trends

While the potential of zero-knowledge proofs is immense, financial institutions must approach adoption with a clear-eyed understanding of the remaining challenges and strategic considerations. A balanced perspective is crucial for navigating the path from exploration to production. Despite the significant progress made, developing secure, efficient, and reliable ZK applications remains a non-trivial undertaking. ZKPs provide powerful tools for privacy, but financial institutions operate within a strict legal framework that mandates disclosure under certain circumstances. Further to this is the reality that successful adoption of any new technology depends not only on its technical merit but also on critical human factors, including talent availability, user acceptance and overcoming institutional inertia and scepticism.

Overcoming scepticism about a new and complex cryptographic paradigm is crucial for building the trust necessary for widespread adoption. This involves clear communication that avoids hype and accurately represents both the capabilities and the limitations of the technology. While challenges remain, a powerful convergence of trends in hardware, software, and standardisation is rapidly accelerating the journey from niche application to mainstream adoption.

While we do not have a crystal ball for the future, this section highlights some of the challenges, trends and themes in the ZKP field and what this might mean for businesses, industry bodies, and regulators. Rulemaking, standardisation, digital assets adoption, and even the development of new technology are all keys to what the future might hold for privacy in payments and financial services.

Challenges

- **High Barrier to Entry:** At its core, ZKP development is a highly specialised field. Designing efficient circuits, optimising performance, and ensuring cryptographic security requires a deep understanding of complex mathematics and cryptography. There is a significant global shortage of talent with this specific expertise, which can make building an in-house team challenging and expensive.
- **Computational Overhead:** The process of generating a ZKP is computationally intensive. This "prover overhead" requires significant processing power and time, which translates directly into operational costs for the entity generating the proofs. While verification is fast, the cost and latency of proof generation can be a major bottleneck for real-time or high-throughput applications, and it remains a key area of ongoing research and optimisation.
- **The Compliance Conundrum:** Regulations such as the Bank Secrecy Act and various AML/CFT directives require institutions to identify customers and report suspicious activity. A ZKP system that provides absolute, unbreakable anonymity may be non-compliant, as it could prevent a firm from responding to a lawful request for information from government authorities or law enforcement.

- **The Need for "Controlled Privacy":** The solution is not to abandon privacy but to design systems that offer controlled disclosure. This involves building mechanisms for authorised access directly into the cryptographic protocol. Examples include using threshold encryption schemes where multiple independent authorities must cooperate to decrypt transaction data or implementing "selective de-anonymisation" functions that can reveal transaction details only when presented with a valid legal warrant. Designing these systems requires a careful balancing of privacy rights and regulatory obligations.
- **Abstracting Complexity for Users:** For all users, ranging from external customers to internal employees, the ZKP technology must be completely invisible. The user experience for a ZKP-powered application must be as simple and intuitive as any traditional application. All the underlying cryptographic complexity must be abstracted away into a seamless interface that builds trust without requiring the user to understand the mathematics.
- **Trade-offs between ZKP methods**: As illustrated by the various use cases, success in a PoC doesn't always mean that the model is scalable, will save money, or that regulations are in place to support further development. Use cases need to be reviewed and updated. Some options might take longer to implement in other jurisdictions owing to the rulebook in that location. Different methods, processes and business appetite will all play a role in the models used for change in financial services ZKP.

A Convergence of Trends

- **Software Abstraction:** The paradigm shift with a zero-knowledge virtual machine (zkVM) is that developers no longer need to write a specific circuit for each specific program they want to prove. Instead, a single, highly optimised, universal circuit is created once for the VM's entire instruction set. After that, any program written in a high-level language, such as Rust, can be compiled into the zkVM's instruction set (bytecode). When this program is executed by the zkVM, the machine automatically generates a ZKP attesting that the execution was performed correctly according to the program's logic. zkVMs almost completely abstract away the need for application developers to understand circuits or constraints. They can write complex, general-purpose applications using familiar languages and toolchains and make them "provable" with minimal ZK-specific knowledge. This dramatically lowers the barrier to entry and expands the potential developer pool from a few hundred specialised cryptographers to many software engineers worldwide.
- **Standardization:** For any technology to achieve widespread enterprise adoption, it needs standards. Industry bodies like ZKProof.org, in collaboration with government agencies like the U.S. National Institute of Standards and Technology (NIST), are actively working to standardise ZKP terminology, security properties, and protocols. This effort will foster interoperability between different ZKP systems, reduce fragmentation, and give enterprises the confidence to invest in technology built on stable, well-vetted foundations. Much like how the standardisation of protocols like HTTP and TCP/IP enabled

the explosive growth of the internet, ZKP standards will pave the way for a new era of trusted digital interaction.

- **Hardware Acceleration:** A primary bottleneck for ZKP adoption has been the high computational cost of proof generation. In response, a specialised industry is emerging to tackle this problem at the hardware level. Companies are designing custom silicon (ASICs) and field-programmable gate arrays (FPGAs) specifically optimised for the mathematical operations core to ZKPs. This hardware acceleration promises to drastically reduce proving times and costs, making ZKP-based systems fast and efficient enough for real-time, high-volume financial applications.

06

The Future of ZKPs in Blockchain Finance

Zero-Knowledge Proofs in Blockchain Finance: Opportunity vs. Reality

The Way Forward: The Future of ZKPs in Blockchain Finance

As we reach the end of this exploration into ZKPs in blockchain fi-nance, it is clear that we are witnessing the emergence of a technology with the potential to fundamentally reshape the financial landscape. The journey through the opportunities, chal-lenges, and real-world applications of ZKPs reveals a field that is relevant to the future of digital assets, privacy, and trust.

From Theory to Practice: Use Cases and Market Examples

The promise of ZKPs is not just theoretical. Across the financial sector, we see concrete use cases and pioneering projects that demonstrate both the power and the complexity of this technology.

- **Private On-Chain Transactions and Asset Managemen**t: Institutions face the dual challenge of leveraging blockchain's transparency while protecting sensitive data. ZKPs enable shielded transactions, where details remain confidential, but compliance is cryptographically enforced. The Bank of England and MIT's digital pound project, as well as the BIS "Tourbillon" initiative, exemplify how privacy and regulatory requirements can be balanced in central bank digital currency (CBDC) designs. These projects show that it is possible to offer a level of cash-like privacy in digital payments, while still meeting anti-money laundering and counter-terrorist financing (CFT) obligations.
- **KYC and AML Verification:** The burden of repetitive, manual identity checks is a longstanding pain point in finance. ZKPs, through self-sovereign identity and verifiable credentials, offer a way to prove identity attributes without exposing underlying personal data. Deutsche Bank's collaboration with Privado ID and Google's partnership with Sparkasse for age verification in digital wallets are real-world examples where ZKPs streamline compliance, reduce data liability, and improve user experience.
- **Proof of Reserves:** In the wake of high-profile exchange failures, the need for transparent, verifiable solvency has never been greater. ZKP-based proof of reserves systems, as implemented by Binance and OKX, allow exchanges to prove they hold sufficient assets without revealing sensitive commercial information or customer data. This shift from "trust me" to "verify me" is a powerful step towards restoring confidence in digital asset markets.
- **Blockchain Scaling Solutions:** As financial institutions look to public blockchains for settlement and innovation, scalability becomes a critical concern. ZKPs underpin technologies like zk-rollups, which allow thousands of transactions to be processed off-chain and verified on-chain with a single succinct proof. The INTMAX2 project, in collaboration with Nethermind and the University of Porto, demonstrates how stateless rollups and advanced cryptographic techniques can deliver both privacy and performance, paving the way for scalable, decentralised finance.

Why This Matters: The Stakes for Blockchain and Financial Services

The importance of ZKPs for blockchain and financial services is rapidly developing as new models emerge. As digital assets become more integrated with traditional finance, the need for privacy, trust, and compliance grows ever more acute. ZKPs offer a rare combination: the ability to prove facts without revealing secrets, to automate compliance without sacrificing confidentiality, and to scale systems without compromising security.

The financial sector stands at a crossroads. Those who embrace the rigorous experi-mentation, collaboration, and innovation required to harness ZKPs will help build a more secure, efficient, and inclusive financial system. Those who hesitate risk being left behind as the digital asset landscape evolves.

In closing, the journey of ZKPs is underway. The opportunities are vast, the challenges real, and the impact—if realised—will be profound. Now is the time for the financial industry to move from exploration to action, to turn the promise of zero-knowledge into the reality of trusted, privacy-preserving digital finance.

07

Appendix: Glossary of Key Terms

Zero-Knowledge Proofs in Blockchain Finance: Opportunity vs. Reality

Appendix: Glossary of Key Terms

This glossary provides concise definitions for the essential terminology used throughout this report, serving as a quick reference for readers.

- **Arithmetic Circuit:** The fundamental representation of a computation for a ZKP system. It consists of a series of gates representing addition and multiplication operations over a finite field.
- **Constraint:** A single mathematical equation (e.g., a×b-c=0) that must be satisfied by the public inputs and the private witness for a proof to be considered valid. A circuit is a system of such constraints.
- **Interactive vs. Non-Interactive Proof:** An interactive proof requires a back-and-forth dialogue of challenges and responses between the Prover and Verifier. A non-interactive proof consists of a single message from the Prover that can be verified by anyone without further communication, which is essential for scalable systems like blockchains.
- **Layer 1:** A layer 1 blockchain is the foundational, base-level infrastructure of a blockchain network, like a mainnet. It handles core functions independently, including processing and finalizing transactions, validating data, and achieving consensus through its own protocol. Examples include Bitcoin and Ethereum.
- **Layer 2:** This refers to any off-chain network, system, or technology built on top of a blockchain to help extend its capabilities.
- **Layer 3:** Layer 3 builds on top of Layer 1 and Layer two technology to support communication between blockchains, leverage off-chain computation (e.g., proof of stake), and offers more functionality and scale.
- **Merkle Tree:** A hash-based tree structure where each leaf represents the hash of a data element and each parent node is the hash of its children. It provides efficient and secure proofs of data inclusion, widely used in blockchains and zero-knowledge proofs.
- **Cryptocurrency Mixer:** A cryptocurrency mixer is a service that combines funds from multiple users to obscure the origin and destination of their coins, making transactions more difficult to trace. These services work by pooling various cryptocurrencies and then redistributing them to users, often for a fee, which can be used for legitimate purposes like privacy-preserving donations or for illicit activities such as money laundering.
- **Prover:** The entity in a ZKP protocol that generates the proof to convince the Verifier of a claim's validity.
- **Succinctness:** A key property of some ZKPs (like zk-SNARKs) where the proof size is very small and the verification time is very short, regardless of the complexity of the original computation being proved.
- **Trusted Setup:** An initial cryptographic ceremony required by certain ZKP systems (notably many zk-SNARKs) to generate public parameters for proving and verifying. This process creates a secret ("toxic waste") that must be destroyed to ensure the system's security.
- **Verifier:** The entity in a ZKP protocol that checks the validity of the proof provided by the Pro

- **Witness:** The secret information (private inputs and intermediate values) known only to the Prover that satisfies the circuit's constraints and is used to generate the proof.
- **zk-DSL (Zero-Knowledge Domain-Specific Language):** A programming language designed to simplify the complex task of writing ZK circuits, allowing developers to work at a higher level of abstraction.
- **zk-SNARK (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge):** A widely used class of ZKPs known for their very small proof sizes and fast verification times. Many variants require a trusted setup.
- **zk-STARK (Zero-Knowledge Scalable Transparent Argument of Knowledge):** A class of ZKPs that does not require a trusted setup ("transparent") and is designed to be highly scalable for very large computations. They are also considered resistant to attacks from quantum computers but typically have larger proof sizes than zk-SNARKs.
- **zkVM (Zero-Knowledge Virtual Machine):** A virtual machine whose correct execution can be proven with a ZKP. It allows developers to write general-purpose programs in standard languages and automatically generate proofs of their correct execution, abstracting away the need to write circuits manually.

08

References

Zero-Knowledge Proofs in Blockchain Finance:
Opportunity vs. Reality

References

1. eIDAS Regulation. https://digital-strategy.ec.europa.eu/en/policies/discover-eidas
2. GENIUS Act. https://www.congress.gov/bill/119th-congress/senate-bill/1582/text
3. Binance. “Proof of Reserves”. https://www.binance.com/en/proof-of-reserves
4. Bank of England and MIT. “Enhancing the Privacy of a Digital Pound with Bank of England”. https://www.dci.mit.edu/projects/enhancing-the-privacy-of-a-digital-pound
5. Deutsche Bank. “Digital Identity”. https://corporates.db.com/files/documents/publications/db-polygo-digital-id-wp-42pp-web-secured.pdf
6. S. Goldwasser, S. Micali, and C. Rackoff. 1985. “The knowledge complexity of interactive proof-systems”. ACM symposium on Theory of computing (STOC '85). Association for Computing Machinery, New York, NY, USA, 291–304. https://doi.org/10.1145/22145.22178. https://dl.acm.org/doi/10.1145/22145.22178
7. Eli Ben-Sasson, et al. “Scalable, transparent, and post-quantum secure computational integrity”. https://eprint.iacr.org/2018/046
8. Satoshi Nakamoto. “Bitcoin: A Peer-to-Peer Electronic Cash System”. 2008. https://bitcoin.org/bitcoin.pdf
9. Jean-Jacques Quisquater, et al. (1990). "How to Explain Zero-Knowledge Protocols to Your Children". Advances in Cryptology (CRYPTO ‘89). Lecture Notes in Computer Science. Vol. 435. pp. 628–631. https://link.springer.com/chapter/10.1007/0-387-34805-0_60
10. Fiat, Amos; Shamir, Adi (1987). "How to Prove Yourself: Practical Solutions to Identification and Signature Problems". Advances in Cryptology (CRYPTO ‘86). Lecture Notes in Computer Science. Vol. 263. Springer Berlin Heidelberg. pp. 186–194. https://link.springer.com/chapter/10.1007/3-540-47721-7_12
11. EDBP. “Guidelines on Processing of Personal Data Through Blockchain Technologies”. 2025. https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-022025-processing-personal-data_en
12. European Union. “General Data Protection Regulation (GDPR)”. https://gdpr-info.eu/
13. Chalkias, K., Chatzigiannis, P., Ji, Y. (2023). “Broken Proofs of Solvency in Blockchain Custodial Wallets and Exchanges”. Financial Cryptography and Data Security (FC 2022). Lecture Notes in Computer Science, vol 13412. Springer, Cham. https://link.springer.com/chapter/10.1007/978-3-031-32415-4_9
14. Reuters. “Trump's digital dollar ban gives China and Europe's CBDCs free rein”. https://www.reuters.com/markets/currencies/trumps-digital-dollar-ban-gives-china-europes-cbdcs-free-rein-2025-01-28/
15. Bank of International Settlements (BIS). “Project Tourbillon - Exploring privacy, security and scalability for CBDCs”. 2023. https://www.bis.org/publ/othp80.pdf
16. Europol. “Criminal finances and money laundering”. https://www.europol.europa.eu/crime-areas/criminal-finances-and-money-laundering
17. Google. Sparkasse Partnership Announcement. https://blog.google/around-the-globe/google-europe/we-are-announcing-sparkasse-as-our-first-national-credential-partner-for-eu-age-assurance/
18. PRNewswire. “OKX's 27th Consecutive Proof of Reserves: $27.9bn in Primary Assets, Audited by Hacken”. https://www.prnewswire.com/news-releases/okxs-27th-consecutive-proof-of-reserves-27-9bn-in-primary-assets-audited-by-hacken-302364040.html
19. INTMAX. https://intmax.io/
20. Aztec Network. https://aztec.network/

09

About us

Zero-Knowledge Proofs in Blockchain Finance:
Opportunity vs. Reality

About us

Nethermind

Nethermind is a blockchain and AI research and software engineering company, empowering enterprises and developers worldwide to work with and build on decentralized and agentic systems. Our work spans the entire blockchain ecosystem, from fundamental cryptography, consensus, and protocol research through security to application-layer protocol development. As a major core contributor to Ethereum and an active builder in the ecosystem, we leverage our deep expertise to provide strategic support to our institutional and enterprise partners across blockchain, AI, and digital assets.

Deutsche Bank

Deutsche Bank provides retail and private banking, corporate and transaction banking, lending, asset and wealth management products and services as well as focused investment banking to private individuals, small and medium-sized companies, corporations, governments and institutional investors. Deutsche Bank is the leading bank in Germany with strong European roots and a global network.

Authors

Antonio Sabado
Chief Growth Officer,
Nethermind

Michal Zajac
Chief Strategy Officer,
Nethermind

Stefano De Angelis
Research Lead,
Nethermind

Joy Adams
COO, Digital Assets & Currencies
Transformation, Deutsche Bank

Sabih Behzad
Head of Digital Assets & Currencies
Transformation, Deutsche Bank

Thomas Brophy
Digital Assets & Currencies
Transformation, Deutsche Bank

Non-Investment Disclaimer

This whitepaper has been prepared for the general information and understanding of the readers. No representation or warranty, express or implied, is given by Deutsche Bank and/or Nethermind as to the quality, accuracy, reliability, adequacy, or completeness of any of the information, material or opinions contained in the above whitepaper. Deutsche Bank and Nethermind expressly disclaim any liability for errors or omissions in such information and material.

This whitepaper is meant for informational purposes only. It is not meant to serve as investment advice. Both past performance and yield may not be a reliable guide to future performance. All information provided by Deutsche Bank and Nethermind is impersonal and not tailored to any subscriber's needs.

Nethermind is not a securities broker/dealer, cryptoasset broker/dealer, investment adviser, commodity trading advisor, or financial adviser, analyst, or planner of any kind. Nethermind is neither licensed nor qualified to provide investment or trading advice, and Nethermind does not explicitly or implicitly recommend or suggest an investment strategy of any kind. Readers should conduct their own research and consult an independent financial, tax or legal advisor before making any investment decision.

Any individual who chooses to invest in cryptoassets should do so with caution. Investing in cryptoassets is speculative and carries a high degree of risk; you may lose some or all of the money that is invested, and if you engage in margin transactions, your loss may exceed the amount invested.

No third party should rely on this whitepaper in any way, including without limitation as financial, investment, tax, regulatory, legal, or other advice, or interpret this whitepaper as any form of recommendation.

Let’s build a compliant and innovative future **together.**

nethermind.io

db.com