

# Project EPIC

Fueling Tokenized Finance with  
On-Chain Enterprise Privacy,  
Identity, and Composability

kinexys  
by J.P.Morgan

# Foreword

Blockchain technology and asset tokenization stand poised to reshape global financial markets, offering unparalleled opportunities for efficiency, transparency and access. At the forefront of this transformation is Kinexys by J.P. Morgan (formerly known as Onyx by J.P. Morgan), our firm's blockchain-focused business unit dedicated to revolutionizing money and asset movement for our institutional and corporate clients.

Within this innovative framework, Kinexys Digital Assets (KDA (formerly known as Onyx Digital Assets (ODA))), J.P. Morgan's digital assets platform has emerged as a pivotal infrastructure, demonstrating practical applications of tokenized assets on blockchain rails. KDA has successfully facilitated trading and settlement activity worth over \$1.5T, enabling clients to leverage traditional assets like US Treasuries, money market funds and fixed income instruments in novel ways. From intraday borrowing through repo to streamlined margin management, KDA is redefining how financial transactions are conducted. As we look to expand the capabilities of KDA, we recognize that on-chain privacy and advancements in identity management are the linchpin for unlocking its full potential for our clients. Enhanced privacy measures are essential for broadening access to the KDA platform and expanding its applications in the financial ecosystem. Streamlined identity management is also a crucial enabler for the scalability of tokenized assets, on KDA and beyond.

Our focus on on-chain privacy and identity is not new. Our journey began in 2017 with the development of the Zero Knowledge Security Layer (ZSL)<sup>1</sup>, a blockchain-agnostic protocol based on zkSNARKs designed by Zcash to enable digital asset privacy. In 2019, we developed Anonymous Zether, a protocol for confidential transactions on the Ethereum blockchain. Throughout the years, the Kinexys Labs (formerly known as Onyx Blockchain Launch) team has consistently championed decentralized digital identity as key to revolutionizing blockchain adoption while delivering transformative blockchain solutions. We publicized this exploration through our collaboration with the Monetary Authority of Singapore, resulting in the "Institutional DeFi: The Next Generation of Finance" report in 2022<sup>2</sup>. We then open-sourced our Self Sovereign Identity Software Development Kit<sup>3</sup> and conducted J.P. Morgan's first external hackathon. More recently, our work with KDA on "The Future of Wealth Management" in 2023<sup>4</sup> continued to push the boundaries of what's possible in financial systems rooted in tokenization, noting on-chain privacy and streamlined identity management as two key challenges to tackle next.

This report serves as a comprehensive examination of Kinexys' perspective on privacy, identity and composability in asset tokenization. Our aim is two-fold: to articulate the challenges and opportunities in this space and to catalyze industry-wide dialogue and action. By sharing our insights and experiences, we hope to foster collaboration and innovation that will drive the next phase of evolution in tokenized finance.

The timing of this report is deliberate, coinciding with our increased focus on fund tokenization for streamlined lifecycle operations and enhanced distribution through 2024 and beyond. As we embark on this next chapter, we believe that addressing the triad of privacy, identity and composability is crucial for realizing the full potential of blockchain in finance.

While this report reflects the collaborative efforts of numerous business and technical contributors through interviews conducted and discussions had, it expressly represents the views of the authors. We invite you to engage with the ideas presented herein, as we collectively work towards a future where digital asset transactions are not only revolutionary in their efficiency but uncompromising in their security and privacy.

**Alexandra Prager**

Head of Kinexys Labs  
Kinexys by J.P. Morgan

**Keerthi Moudgal**

Head of Product, Kinexys Digital Assets  
Kinexys by J.P. Morgan

**Nikhil Sharma**

Head of Growth, Kinexys Digital Assets  
Kinexys by J.P. Morgan

# Contents

<b>Foreword</b>	<b>2</b>
<b>From Billions to Trillions: Privacy and identity as catalysts for asset tokenization</b>	<b>6</b>
<b>Investment Funds: Opportunities and challenges within tokenization</b>	<b>12</b>
<b>Technical Deep-dive: On-chain privacy &amp; digital identity</b>	<b>18</b>
<b>Requirements and Evaluation: Defining the use cases</b>	<b>32</b>
<b>Findings</b>	<b>34</b>
<b>Conclusion and Future Outlook</b>	<b>39</b>
<b>Appendix: Case Studies</b>	<b>41</b>
Kinexys by J.P. Morgan’s implementation leveraging Zama’s privacy solution	41
AvaCloud Privacy Solutions	46
Fhenix Privacy Solutions	49
Global Technology Applied Research, JPMorgan Chase -- Private, Auditable and Distributed Ledger (PADL)	52
Rayls by Parfin Privacy Solutions	57
<b>References</b>	<b>61</b>

## Authors:

### Alexandra Prager

Head of Kinexys Labs  
alexandra.n.prager@jpmorgan.com

### Keerthi Moudgal

Head of Product, Kinexys Digital Assets  
keerthi.moudgal@jpmorgan.com

### Nikhil Sharma

Head of Growth, Kinexys Digital Assets  
nikhil.b.sharma@jpmchase.com

### Dennis Cristallo

Head of Wealth Management,  
Kinexys Digital Assets and Kinexys Labs  
dennis.cristallo@jpmorgan.com

### Joe Leung

Privacy Lead & Senior Technical Product  
Manager, Kinexys Digital Assets  
joe.leung@jpmorgan.com

### George Kassis

Web3 Identity Lead & Senior Product Manager,  
Kinexys Labs  
george.kassis@jpmorgan.com

### Brody Wacker

Growth, Kinexys Digital Assets  
brody.wacker@jpmorgan.com

### Stephanie Lok

EPIC Lead & Product Manager,  
Kinexys Digital Assets  
stephanie.lok@jpmorgan.com

### Bipin Mathew

Product Manager, Kinexys Digital Assets  
bipin.mathew@jpmorgan.com

### Patricia Jaimez Gómez

Web3 Identity Product Manager, Kinexys Labs  
patricia.jaimezgonzalez@jpmorgan.com

### Alethea Tan

Growth Analyst, Kinexys Digital Assets  
alethea.tan@jpmorgan.com

### Dylan Paul

Product Analyst, Kinexys Labs  
dylan.paul@jpmorgan.com

## Contributors:

### Sudhir Upadhyay

Head of Engineering, Kinexys by J.P. Morgan  
sudhir.x.upadhyay@jpmorgan.com

### Manmeet Ahluwalia

Head of Engineering, Kinexys Digital Assets  
manmeet.ahluwalia@jpmchase.com

### Imran Bashir

Principal Software Engineer,  
Kinexys by J.P. Morgan  
imran.m.bashir@jpmorgan.com

### Jitendra Bhurat

Senior Lead Software Engineer,  
Kinexys Digital Assets  
jitendra.bhurat@jpmorgan.com

### Angela Pratt

Lead Software Engineer, Kinexys Labs  
angela.pratt@jpmchase.com

### Ganesh Anantwar

Lead Software Engineer,  
Kinexys Digital Assets  
ganesh.anantwar@jpmchase.com

### Abhishek Agarwal

Software Engineer III, Kinexys Digital Assets  
abhishek.x4.agarwal@jpmchase.com

### Alexandros Mylonas

Software Engineer III, Kinexys Labs  
alexandros.mylonas@jpmorgan.com

### Shaltiel Eloul

Applied Research Director,  
Global Technology Applied Research  
shaltiel.eloul@jpmchase.com

### Shawn Roling

Design Lead, Kinexys by J.P. Morgan  
shawn.m.roling@jpmchase.com

### Jack Nicholson

Senior Designer, Kinexys by J.P. Morgan  
jack.x.nicholson@jpmorgan.com



Securities Services &  
Global Technology Applied Research

# From Billions to Trillions: Privacy and identity as catalysts for asset tokenization

The asset tokenization market, currently valued in billions, is poised for exponential growth, with industry analyses from leading consulting firms projecting a multi-trillion dollar future. However, realizing this transformative potential hinges critically on addressing institutional-grade privacy and developing composable, privacy-preserving identity solutions. Without these foundational elements, the industry's expansion will remain constrained, particularly in attracting traditional investors who expect robust data protection comparable to conventional markets.

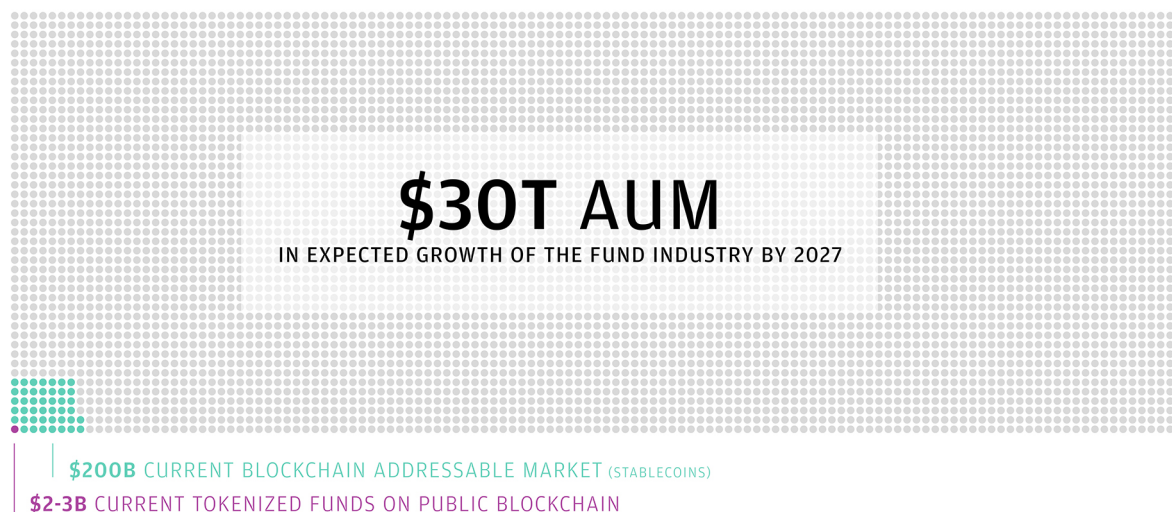
At Kinexys Digital Assets, we have been at the forefront of implementing tokenization in traditional financial flows, successfully processing \$2-3B worth of tokenized asset transactions daily. Our decision in 2020 to build on an Ethereum Virtual Machine (EVM<sup>5</sup>)-based permissioned blockchain has been validated by the remarkable growth within the Ethereum and EVM ecosystems. This strategic choice leverages blockchain's inherent characteristics: immutability, trust-minimization, transparency, programmability and decentralization. Using these constructs, KDA's current solutions effectively mitigate settlement risk, automate trade and asset lifecycle management and streamline reconciliation efforts, attracting numerous peers and clients to our platform.

Separately, the institutional landscape has evolved significantly over the past year, with increased activity on public blockchains driven by asset managers<sup>6</sup>, as evidenced by rising assets under management (AUM) in on-chain investment products. While operational efficiency remains a key driver, there is a notable emphasis on accessing new distribution channels, particularly focusing on crypto-native investors.

Regardless of whether assets are tokenized on public or permissioned chains, or whether the immediate focus is operational optimization or distribution expansion, traditional market requirements remain unfulfilled. The lack of mature, on-chain cryptographic privacy solutions, coupled with the absence of consensus on implementing privacy-preserving digital identity, continues to create operational friction in tokenized asset interactions. While these challenges are not entirely gating - as demonstrated by the \$2-3B<sup>7</sup> raised through on-chain funds and approximately \$200B<sup>8</sup> in stablecoins, protocol treasuries and public chain lending protocols, solving for them could broaden adoption.

Current market activity on public blockchains demonstrates demand from participants for whom robust privacy and industry-wide identity solutions may be less critical. However, for traditional investors, data privacy is a baseline requirement, and without comprehensive, yet seamless privacy and digital identity solutions, key benefits of tokenization will remain unrealized.

## Funds Addressable Market



\*For illustrative purposes. See report for source details

Boston Consulting Group projects global assets under management to grow by \$30T over the next three years<sup>9</sup>. We believe a significant portion of this growth could materialize in tokenized form, provided traditional investors have the necessary comfort, confidence and tools to participate in the tokenized ecosystem.

## Our Vision

We envision a future where all parties can transact, build and benefit within public and permissioned ecosystems efficiently and privately. Success of this vision is hinged on:

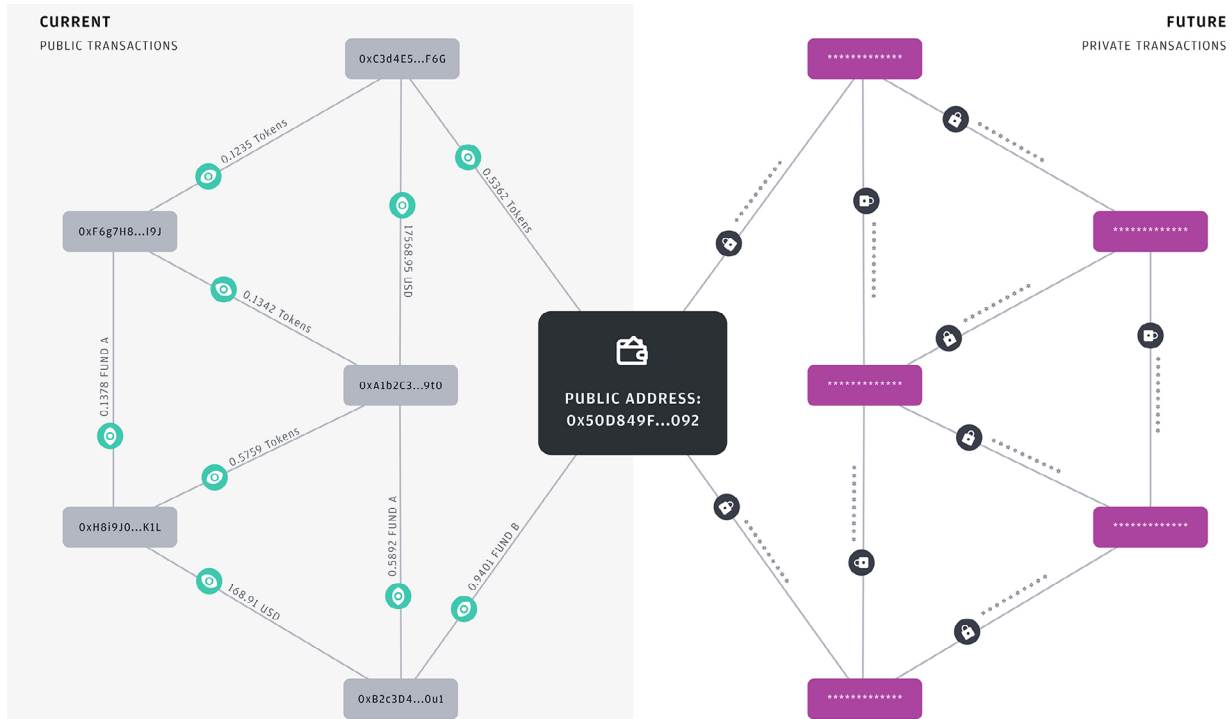
### 1 Solving for Privacy: Where Transparency and Confidentiality Coexist On-Chain

**Current state:** Most public blockchains are transparent and permissionless. Anyone with the right infrastructure can run a node and validate transactions, while anyone with internet access can view transactions, balances, and the mechanics of smart contracts. Permissioned networks may employ operational privacy to meet client needs, (e.g. KDA uses access controls), however, this comes at the cost of a constrained ability to distribute infrastructure and minimize trust among participants.

This openness is a double-edged sword, offering the benefit of transparency at the cost of privacy. While on-chain addresses appear random and unattributable, they are pseudonymous and do not guarantee anonymity.

**Target state:** Participants should have the choice to shield important details and protect sensitive financial information. In such a state, data would be conditionally disclosed on a unified ledger with a shared state, ensuring transparency without compromising confidentiality.

# On-chain Transaction Visibility



## 2 Solving for Identity: Compliance is Streamlined

**Current state:** The absence of standardized approaches and infrastructure among market intermediaries for identity verification and compliance creates significant inefficiencies in asset interactions. Even with tokenized assets, this lack of standardization leads to redundant processes, diminishing the operational benefits that tokenization promises to deliver.

- **Trustworthiness of Identity:** Identity attributes (e.g. Know Your Customer (KYC) status) are only as reliable as the trusted entity that made the attestation. For example, the New York Department of Motor Vehicles (DMV) is a trusted governmental entity who can attest to an individual’s name and address.

While there are analog systems for validating such trusted entities, these systems are not intrinsically compatible or integrated with blockchain networks. Additionally, the absence of consistent trust frameworks across financial market participants prevents the efficient reuse of compliance and onboarding verifications.

- **Challenges with Storing Personally Identifiable Information (PII) On-Chain:**

Storing PII on a shared ledger compromises privacy and security, making it potentially unsuitable for regulated financial applications. The key challenge is ensuring that an on-chain actor acquires relevant attestations and identity checks without revealing any PII.

**Target state:** Repurposable digital identities could revolutionize KYC and Anti-Money Laundering (AML) processes. Investors could efficiently verify their identities across multiple platforms and use cases, significantly reducing redundancy and enhancing the user experience while maintaining robust compliance standards.



### 3 The Preservation of Composability is Paramount

Composability refers to the ease with which different elements of a system can be combined to create new components altogether. Financial markets are inherently composable, even in the absence of blockchain technology. A prime example is an investment fund, which is a wrapper, or structure, predicated upon investments and capital flow into other assets.

Blockchain and tokenization serve as catalysts to improve upon the composability of finance in the below ways:

- 1 By enabling the conversion of financial assets and processes into modular, reusable code
- 2 By driving automation in the execution of operational processes

Once an asset is tokenized, it is much easier to move, settle, and service. The asset could also be used in purpose-built applications: e.g. applications for financing, secondary trading, collateralization, and more, which further enhances asset utility. The EVM ecosystem, with over 2,000 protocols<sup>10</sup>, is a key proof point in the rapid acceleration of growth and financial innovation that modularity and autonomy can bring.

Well-designed privacy and digital identity solutions can complement and thoughtfully enhance composability and amplify value creation across the ecosystem (see diagram on next page).

## Purpose of this Report

Our first step to realize our vision around enterprise privacy, identity, and composability was to conduct a proof of concept (POC) initiative with four key objectives:

- 1 Validate institutional needs around privacy and identity
- 2 Identify criteria required for a scalable identity solution
- 3 Explore the viability of nascent privacy solutions in market today
- 4 Bring together institutional & web3-native worlds to find a viable path forward

We anchored this exploration to real business problems within the investment funds ecosystem, ensuring our analysis remained grounded in practical utilities.

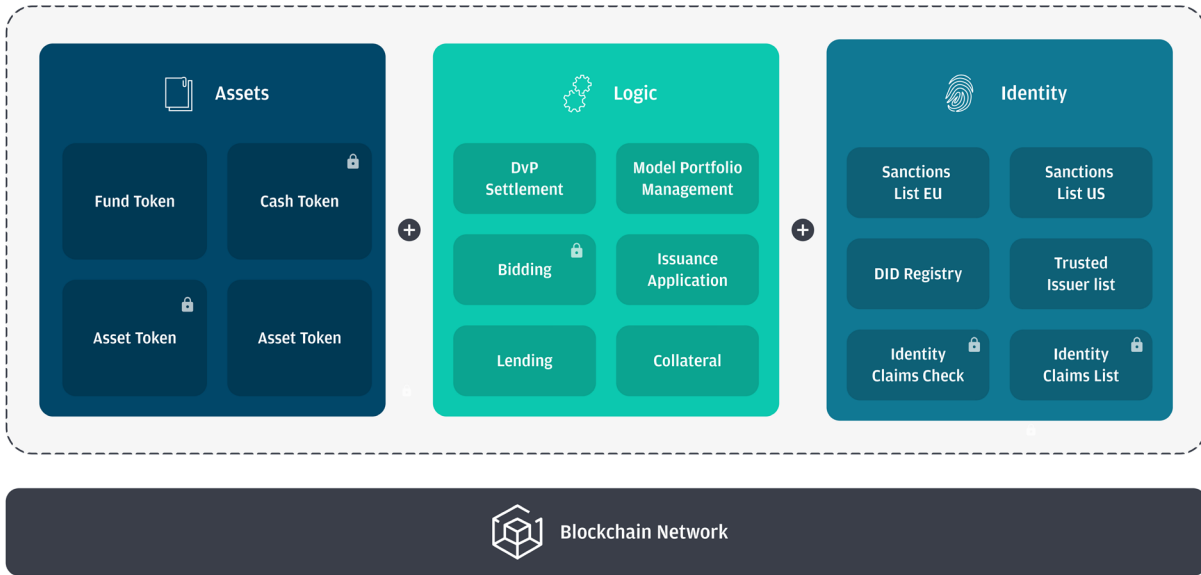
This POC builds on past initiatives, including our 2023 report on The Future of Wealth Management<sup>11</sup>, where we showcased the transformative power of managing entire portfolios of tokenized investments using smart contracts. Our findings showed that roughly ~3,000 steps could be collapsed into a few clicks, that end investors could benefit from the elimination of cash drag and that this technology could help asset managers realize the \$400B annual incremental revenue opportunity<sup>12</sup> in better serving high net worth investors. Importantly, this work highlighted the need for scalable privacy solutions and robust identity frameworks to enable such transformation at scale.

# 1 Components of Composable Financial Ecosystems

LEGEND

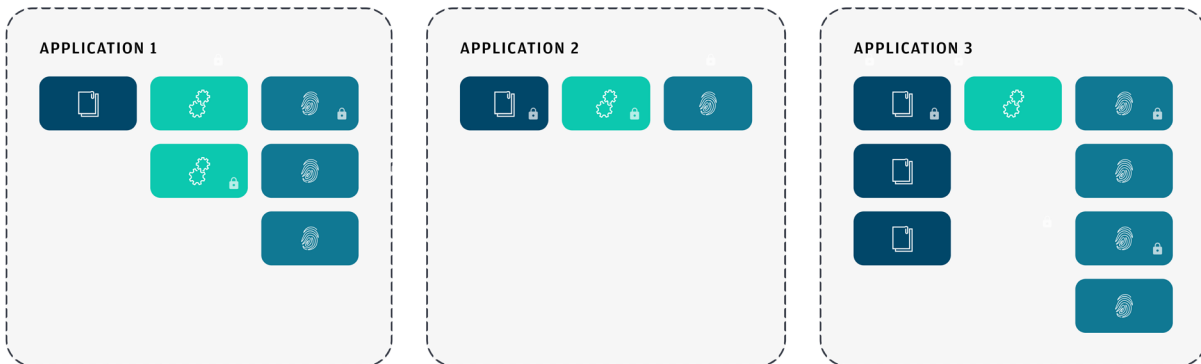
🔒 Private

Business applications and solutions are comprised at a high level of a combination of assets, logic and identity mechanisms



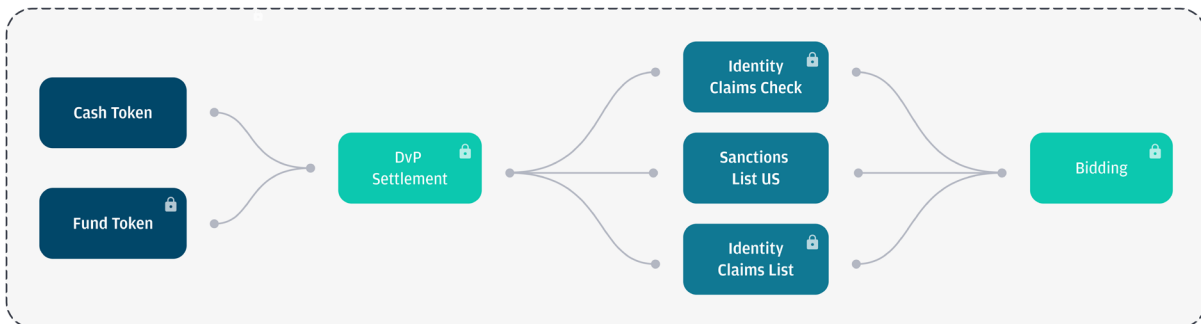
# 2 Structured Reusable Components

Once deployed on-chain, these components serve as building blocks for the construction of new applications



# 3 Illustrative Business Case

For example, an auction application can be built on top of existing assets and cash which plugs into bidding logic to complete auction and subsequent settlement, all while leveraging pre-existing on-chain contracts for identity checks



Although our POC centers on the investment funds ecosystem, our learnings extend to several asset classes beyond just funds. The investment funds lifecycle exemplifies industry-wide inefficiencies that blockchain can address, including manual processes, lack of transparency, and high operational costs. We focused on three progressive use cases: investor onboarding, settlement, and secondary trading within tokenized funds—demonstrating how each use case built on the previous one. An important element for us was to ensure that our use cases could demonstrate the preservation of composability whilst maintaining adherence to institutional needs.

Through structured interviews with Apollo, Albourne Partners Limited, Azalea Asset Management Pte. Ltd, Formidium, J.P. Morgan Securities Services, NAV Fund Services, Schroders, and University of Cambridge Investment Management, we validated the problem statements, needs, and requirements across all types of participants within the fund lifecycle. Against this backdrop, we then explored two key themes, spanning several solutions:



**Privacy-Preserving Technologies:** Zero-Knowledge Proofs (ZKP), Fully Homomorphic Encryption (FHE), and data isolation techniques offer promising solutions to shield identities and asset types, protecting sensitive financial information while maintaining necessary transparency.



**Privacy-Preserving Repurposable Identity:** Decentralized Identifiers (DIDs) provide a framework for managing identities securely and privately, crucial for AML/KYC compliance without compromising investor confidentiality.




The Technical Deep-dive: On-chain privacy & digital identity section provides a deeper exploration of these concepts.

Our technical evaluation phase involved structuring a set of requirements to demonstrate our use cases and themes pertaining to institutional needs, and then implementing these requirements using Zama's FHE solution and the Kinexys Self Sovereign Identity (SSI) SDK. Our Applied Research team, Fhenix, AvaCloud and Parfin also implemented the same requirements.

Finally, we analyzed findings across all implementations to assess the readiness of currently available solutions and identified gaps that need to be bridged for institutional adoption. We have detailed these findings and their implications in the following sections of this report.

# Investment Funds: Opportunities and challenges within tokenization

The complex ecosystem of registered and alternative investment funds comprises various participants, each grappling with distinct challenges that impede efficiency and innovation.

 <p><b>FUND MANAGERS</b></p> <p>Oversee and manage investment portfolios in accordance with a stated strategy</p>	 <p><b>FUND ADMINISTRATORS / TRANSFER AGENTS<sup>1</sup></b></p> <p>Maintain records of investor accounts and facilitating capital activity and transfers as a service provider to the fund manager</p>	 <p><b>INSTITUTIONAL INVESTORS &amp; ALLOCATORS</b></p> <p>Organizations that invest on behalf of their stakeholders or clients to achieve their unique objectives</p>
<p><b>PRIVACY</b></p> <p>Privacy of transactions and positions is expected</p> <p>Lack of privacy introduces competitive and business risks</p> <p>Want to ensure protection of proprietary trading algorithms and asset allocation</p>	<p><b>PRIVACY</b></p> <p>Expected to keep ownership records private and comply with data privacy regulations for clients</p>	<p><b>PRIVACY</b></p> <p>Privacy of transactions and positions is expected</p> <p>Full transparency would increase visibility on fees, asset raising and redemption activity for investors and their stakeholders</p>
<p><b>IDENTITY</b></p> <p>Looking for streamlined/faster investor onboarding, subscriptions and redemptions</p> <p>Compliance with data protection and privacy regulations from all jurisdictions is paramount</p>	<p><b>IDENTITY</b></p> <p>Need for more efficient KYC/AML processes</p> <p>Willing to engage with highly trusted institutions on interoperability</p>	<p><b>IDENTITY</b></p> <p>Looking for more efficient, standardized processes for AML/KYC - although package is generally standardized for institutions</p>
<p><b>TOKENIZATION</b></p> <p>Regulatory compliance is of utmost importance</p> <p>Enables distribution (if user experience excels)</p> <p>Interest in exploring improved secondary markets and ability to provide LPs with leverage</p>	<p><b>TOKENIZATION</b></p> <p>Tokenization creates potential operational efficiencies</p> <p>Client discussions around liquidity and distribution</p>	<p><b>TOKENIZATION</b></p> <p>Improved liquidity and portfolio construction/management capabilities enabled by simplified transfers/secondaries</p> <p>Decreased settlement times</p>

<sup>1</sup> - Throughout this paper we will refer to transfer agents as the actor responsible for investor onboarding. We recognize that for many alternative investment funds transfer agency is offered as part of a fund administrator's bundled service.

“Fund tokenization can improve investor onboarding efficiency by up to 60%. Additionally, making KYC reusable can boost onboarding efficiency to as much as 90%.”

**Nilesh Sudrania, Founder and CEO, Formidium**

---

## Potential Benefits of Fund Tokenization

The investment funds industry, representing \$98T<sup>13</sup> in assets under management, has evolved significantly since the inception of the first open-end fund a century ago<sup>14</sup>. Through continuous innovation, the industry has delivered substantial value to end investors by reducing costs through ETFs and economies of scale, expanding access to alternative investments through innovative structures and enhancing transparency through regulatory reforms and investor advocacy. However, despite these advances, the industry faces meaningful operational inefficiencies characterized by laborious onboarding, siloed systems, manual processes, and high costs.

To continue this trajectory of innovation, the industry must now modernize its fundamental infrastructure.

Blockchain technology and tokenization present a compelling evolution of traditional fund operations.

By leveraging a shared, immutable ledger and smart contracts, the fund industry stands to gain significant advantages in efficiency, transparency, liquidity, and accessibility. Using a blockchain ledger as a unified source of truth can significantly reduce manual reconciliation efforts arising from siloed systems and disparate data structures. Smart contracts can automate repetitive tasks, including AML/KYC checks and cash movement for capital events, potentially enabling fund managers to lower investment minimums and achieve greater economies of scale.

The tokenized asset landscape has evolved significantly, with approximately \$13B in traditional assets currently tokenized on public blockchain networks<sup>15</sup>. While this represents less than 0.01%<sup>16</sup> of industry assets Under management (AUM), adoption is accelerating, with AUM in on-chain products nearly tripling since early 2024. Early adopters are pursuing tokenization to realize operational efficiencies, reduce investment minimums and expand distribution to new investor segments. However, widespread institutional adoption will require robust solutions for privacy and identity management that provide the comfort and confidence traditional investors expect from financial markets.

The immutable nature of blockchain ensures that all fund transactions are recorded transparently on a unified ledger visible to authorized participants, with chronological recordation through consensus mechanisms. This shared source of truth results in improved capital event tracking, reduced disputes from data discrepancies, and enhanced oversight capabilities. Recent implementations demonstrate significant cost reductions, Franklin Templeton reported that processing 50,000 transactions through blockchain would cost \$1.52 compared to \$50K using legacy systems<sup>17</sup>. Similarly, Hamilton Lane's implementation of DLT-share-classes has reduced investment minimums from \$2M to \$10K<sup>18</sup>, demonstrating tangible benefits of tokenization.

Pioneering asset issuers are actively launching and managing tokenized funds to:



### REDUCE OPERATING COSTS

Franklin Templeton cited reducing transfer agency costs from \$50,000 per 50K transactions in the legacy system to \$1.52 total. <sup>1</sup>



### LOWER INVESTMENT MINIMUMS

Hamilton Fund launched a tokenized feeder into their Senior Credit Opportunities Fund, reducing the investment minimum from \$2 million to \$10,000. <sup>2</sup>



### ENHANCE UTILITY OF FUND UNITS

Dozens of fund managers submitted proposals to manage \$1 billion of MakerDao's reserves in tokenized MMFs. These allocations serve as backing for the Dai stablecoin which is widely used in DeFi. <sup>3</sup>

1. <https://blockworks.co/news/tokenization-updates-rwa-summit>

2. <https://www.hamiltonlane.com/en-us/news/scope-available-via-securitize>

3. <https://finance.yahoo.com/news/makerdaos-1b-tokenized-treasury-investment-164345459.html>

## Privacy Considerations

Reasons to preserve privacy of transactions, positions and balances in tokenized products include:

- 1 Alpha Protection:** Asset allocators like institutional investors, wealth managers, fund-of-funds, and OCIO platforms<sup>19</sup> want to protect the confidential contents of their discretionary portfolios which serve as a source of competitive advantage.
  - Public real-time disclosure of portfolio contents could enable competitors to replicate strategies, thereby commoditizing offerings and eroding the manager's ability to charge for this value-add. We would contrast this level of transparency with public pension filings and 13-Fs<sup>20</sup> which are meaningfully lagged, limiting their usefulness for "front-running".
  - Similarly, full transparency on fund subscriptions could lead market participants to deploy capital into a fund's known holdings, degrading the fund's entry point and alpha. One could imagine a sizable tokenized fund specializing in a particular sub-industry, like autonomous vehicles. If investors could see—in real-time—a large subscription into this fund, they could potentially buy the known holdings ahead of the actual fund, pushing up the price in the process.
- 2 Preventing "Runs" on Funds:** Full transparency on redemptions could lead to escalating redemptions, creating a run on the fund.
  - In traditional markets, sudden large redemptions can signal trouble, prompting other investors to redeem their shares to avoid being left with less liquid assets. This can create a self-fulfilling prophecy, where the fear of illiquidity leads to actual illiquidity, destabilizing the fund. For tokenized funds, this process could accelerate, meaning fund managers would have less time to sell assets in an orderly manner, potentially leaving the remaining investors with the least liquid holdings.

“Both managers and allocators have significant sensitivity around privacy, particularly concerning redemption, subscription and co-investment activities.”

**Steven D’Mello, Partner, Operational Due Diligence, Albourne Partners Limited**

---

**3 Ensuring Investor Privacy:** Fund managers and investors of all types (large and small, institutions and individuals) should have the ability to transact privately. In fact, many jurisdictions are legislating these privacy protections through laws like the EU’s General Data Protection Regulation (GDPR), Singapore’s Personal Data Protection Act (PDPA) and the California Consumer Privacy Act (CCPA).

- Investors will prefer privacy for a variety of reasons ranging from personal preference and professional convenience to potential financial consequences that come from signaling to the marketplace buying and selling activity.
- Similarly, fund managers may not be comfortable with their client lists being publicly available. Even with pseudonymous blockchain addresses, we believe if there is a meaningful financial incentive to identify the owner of the wallet, a savvy actor will do so.

**4 Managing Relationships:** Bringing the entire fund lifecycle on-chain could complicate the relationship between fund managers and investors.

- Fully transparent ownership ledgers and fees paid on-chain could add more scrutiny to fund manager fees and how they allocate scarce capacity amongst their investors.
- Similarly, investors may not want fund managers to know the extent of their relationships with competitive firms.

## Identity Considerations

Pragmatic approaches, standardized identity frameworks and automated identity verification would go a long way in streamlining the current onboarding processes in the fund ecosystem.

Regulatory requirements mandate that regulated entities verify investor identities and key attributes to prevent money laundering and other illicit activities, placing the ultimate responsibility on fund managers, who often delegate this task to transfer agents. It is expected that transfer agents maintain strict confidentiality of identity attributes, ensuring that sensitive information is kept private and secure.

“We have to figure out a way to be able to apply some of the KYC and AML practices that exist in traditional finance to tokenization...but we also need to be able to preserve privacy.”

**Robert Mitchnick, (Digital Assets, BlackRock)**

---

For transfer agents, the AML/KYC process is laborious. On average, global financial institutions have 1,566 employees involved in the AML/KYC process resulting in an average cost of \$2,598 per client onboarding<sup>21</sup>. For some investors and managers, onboarding can be fairly straightforward, but for transfer agents who are verifying the identity of thousands of investors in more than 100 countries it hardly feels that way.

Identity verification involves extensive processes, case-by-case evaluations, constant adaptation to evolving regulations and country-specific requirements. The high volume of communication required for risk ratings, beneficiary identification and sanction screening adds further complexity. Moreover, investors could be required to prove document authenticity through cumbersome means such as presenting original documents or obtaining official stamps and/or certified copies.

The process is also highly duplicative with investors having to onboard to each manager relationship, even if the managers are working with the same transfer agent, collecting the same documentation. In order for a transfer agent to re-use information that a given investor has submitted for identity verification—for instance, when that same investor is onboarding onto another fund—the transfer agent may need self-directed consent from the investor.

## Improving Trust, Interoperability and Incentives

Establishing trust and incentives in the identity verification process represents an opportunity for investors, fund managers, and transfer agents.

AML reliance letters provide a potential primitive example for the way forward. These letters are generally provided by fund distributors or another regulated entity attesting that they have conducted the AML/KYC of their clients and that the fund should trust this firm on the basis that they are a regulated entity in good standing. The decision on whether to accept this letter is based on a number of factors including the trustworthiness of the entity, its track record regarding AML/KYC violations, the regulatory regime in which it operates, willingness to provide periodic verification of underlying investors, and/or submit to an audit or sampling of their AML/KYC process.



# “KYC and AML processes are repetitive, often conducted multiple times with the same Investors.”

**Mike Stevens, Transfer Agency Product Manager at J.P. Morgan**

---

Unfortunately, reliance letters only modestly lessen the burden on the ecosystem. They are not universally accepted, nor owned by investors themselves, and they are not linked to the underlying investor data and attributes (e.g. investor type, accreditation status). Further, while transfer agents are the entities generally performing the investor review, the data is not actually theirs. It is being provided to them as a service provider to the fund or fund manager. As such, for the transfer agent to be able to use this information with another fund manager, they would need the consent of the investor.

We recognize the risk of missteps in this space can be costly, however, we plan on continuing our exploration from a viability and incentives perspective. We imagine that a network of like-minded institutions across transfer agents, fund managers, distributors, banks and broker dealers could be assembled to develop digital-first standards and processes on investor identity embodied in a decentralized identification construct similar to what we built in this POC. This network of trusted parties could be incentivized to provide identity verification as a service by charging for the use of these credentials.

Payment for identity verification could roughly parallel the additional charge that some providers impose for AML/KYC or investor accreditation checks today. We believe it could also be designed in a way that leverages the underlying investor attributes to automate some of the manually monitored fund limits. For example, this data and smart contract-based rules could ensure that ERISA<sup>22</sup> investors' ownership remains below the regulatory threshold, currently at 25% of the fund.

## Composability Considerations

Although 'improved liquidity' is a frequently cited benefit derived from tokenization, our view is that simply tokenizing an asset does not make it more liquid—though it does make the asset more composable. For instance, shares of a tokenized investment fund may be operationally easier to utilize in financing, lending and trading applications than those held on a traditional ledger.

## A Demonstration of Composability through Privacy-Preserving Secondary Markets

Among various composable applications that tokenization could enable, several of our interviewees emphasized the potential for mature secondary markets for illiquid fund investments. There are several barriers in place which have prevented more liquid markets for currently illiquid assets from developing including poor user experience,

negotiating purchase/sale terms, non-disclosure agreements and the settlement process. While not all of these issues are solved by technology, we believe that on-chain composability, coupled with robust privacy and identity solutions, could reduce many of these barriers, and lay the groundwork toward more efficient secondary markets.

Today, secondary transactions in illiquid assets are bilaterally negotiated between sellers, buyers, and various intermediaries. The process can be lengthy and manual, with the onboarding, AML/KYC and investor accreditation status of the buyer becoming a critical late-stage barrier that could be solved with a robust digital identity framework. The result is that the market for smaller secondary transactions (< \$2M) is sparse.

Sellers are generally seeking to exit positions to improve liquidity, eliminate an investment line item, or to rebalance. Because the marketplace is not particularly deep or organized, these positions are generally sold at a discount to net asset value. This dynamic can be problematic for fund managers who are marking funds at a higher valuation than they are priced in the secondary market. In a public blockchain setting, discounted sales could create problems for fund managers by increasing redemption/sell pressure and impacting their ability to raise capital for future funds.

We imagine a scenario where a secondary market application can be built upon tokenized funds. The smart contracts—or software—utilized to implement the application could programmatically enforce that only investors with verified AML/KYC credentials can bid on an illiquid asset, increasing settlement speed.

## Technical Deep-Dive: On-chain privacy and digital identity

### On-Chain Privacy and Off-Chain Privacy

A key distinction in blockchain privacy is whether the solution is on-chain or off-chain. Off-chain privacy is achieved through methods like data segregation, access controls, sub-ledgers, and trusted execution environments. Today, many private blockchains, including KDA, use one or more off-chain privacy techniques. While effective, these methods can compromise blockchain benefits. For example:

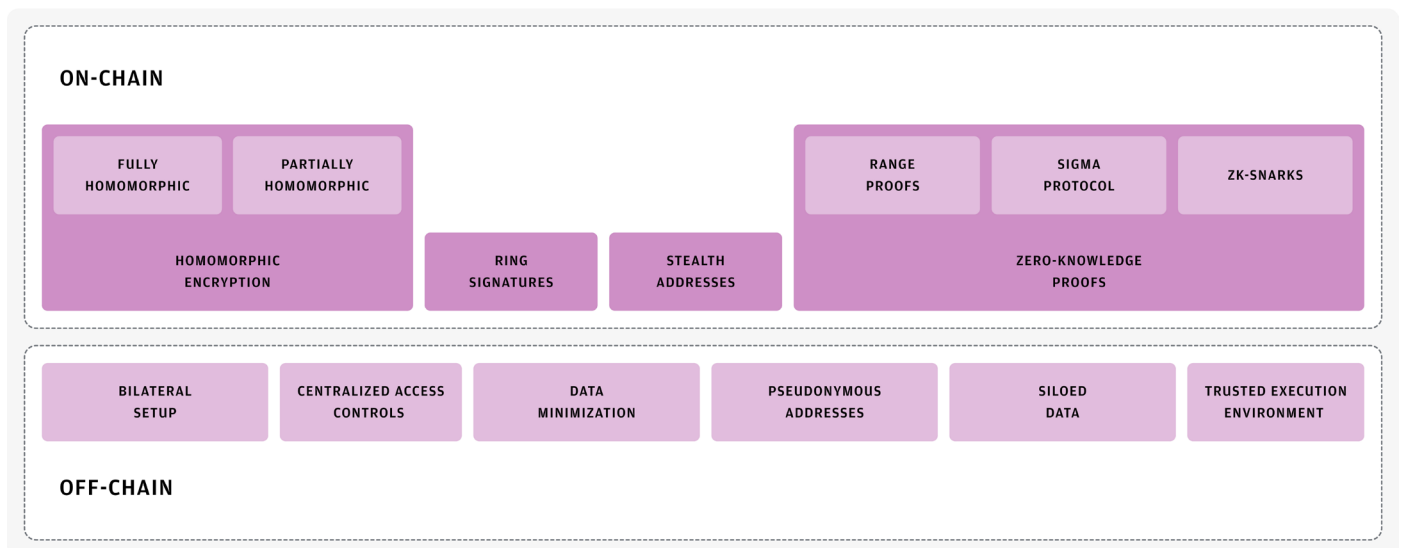
- Access controls, such as UI or API-driven entitlements, impede a network's ability to decentralize or allow participants to directly access node infrastructure. This significantly impacts the benefits that the technology promises.

- Siloed data architectures, unless supported by specialized software solutions, which may themselves reduce trustlessness and decentralization, are not able to easily propagate network-wide features, including interoperability and other innovations. Additionally, network scalability may be hindered by the need for point-to-point connections.
- A Trusted Execution Environment (TEE) provides a secure area within hardware to protect data and computations. While this enhances security by keeping operations confidential, it also limits transparency and decentralization. This reliance on hardware-based security may also introduce concerns about central points of failure or trust in the hardware provider, potentially reducing the overall trustlessness of the blockchain system.
- Private channels may protect information but undermine the blockchain’s role as a single source of truth, potentially requiring trusted intermediaries or complex manual reconciliations in disputes or synchronization failures.

On-chain cryptographic privacy ensures that even with full ledger access, an observer cannot discern transaction details or addresses, and therefore cannot discern identities. This is achieved by integrating privacy mechanisms directly on-chain, either at the protocol level (Zcash) or smart contract level with privacy pools<sup>23</sup>, using techniques including, but not limited to, ZKPs and FHE. On-chain privacy, ideally, isn’t reliant on trusted intermediaries or manual processes, the privacy solutions themselves are often freely scrutinized since they are created using public cryptographic research.

This report explores a number of on-chain and off-chain privacy techniques, which can be used in tandem. Importantly, any privacy solutions applied would, preferably, not erode the core benefits of using blockchain including efficient settlement, reduced reconciliations, trust-minimization, a shared ledger, transparency, decentralization, and programmability.

## Types of Privacy Solutions



# What is On-Chain Privacy?

On-chain privacy, for institutions, can be characterized in three dimensions:

- 1 Anonymity:** Shielding the on-chain accounts and by extension the identities, of the parties involved in a transaction, from anyone outside of the transaction.
- 2 Confidentiality:** Shielding the asset type and quantity being transacted from anyone outside of the transaction.
- 3 Auditability:** Ensuring transactions adhere to regulatory requirements without over-exposing sensitive data. Depending on the context of the transactions, this may involve granting select actors—outside of the transaction—the ability to identify the parties involved, permit, or deny the transaction prior to execution, and to maintain records for audit purposes.

## Our Privacy Focus

KDA uses an Ethereum Virtual Machine (EVM) based blockchain so our focus remains on EVM-compatible techniques. Additionally, we see continued and significant innovation in the Ethereum ecosystem and while there are a broad range of privacy techniques available, we narrowed our scope to some of the more prominent approaches in the EVM ecosystem. For the purposes of bounding our POC scope, we chose to focus on ZKPs, stealth addresses and FHE. The smart contract, or software, utilized to implement the application could programmatically enforce that only investors with verified AML/KYC credentials can bid on a particular asset, increasing settlement speed.

## Zero-Knowledge Proofs (ZKPs)

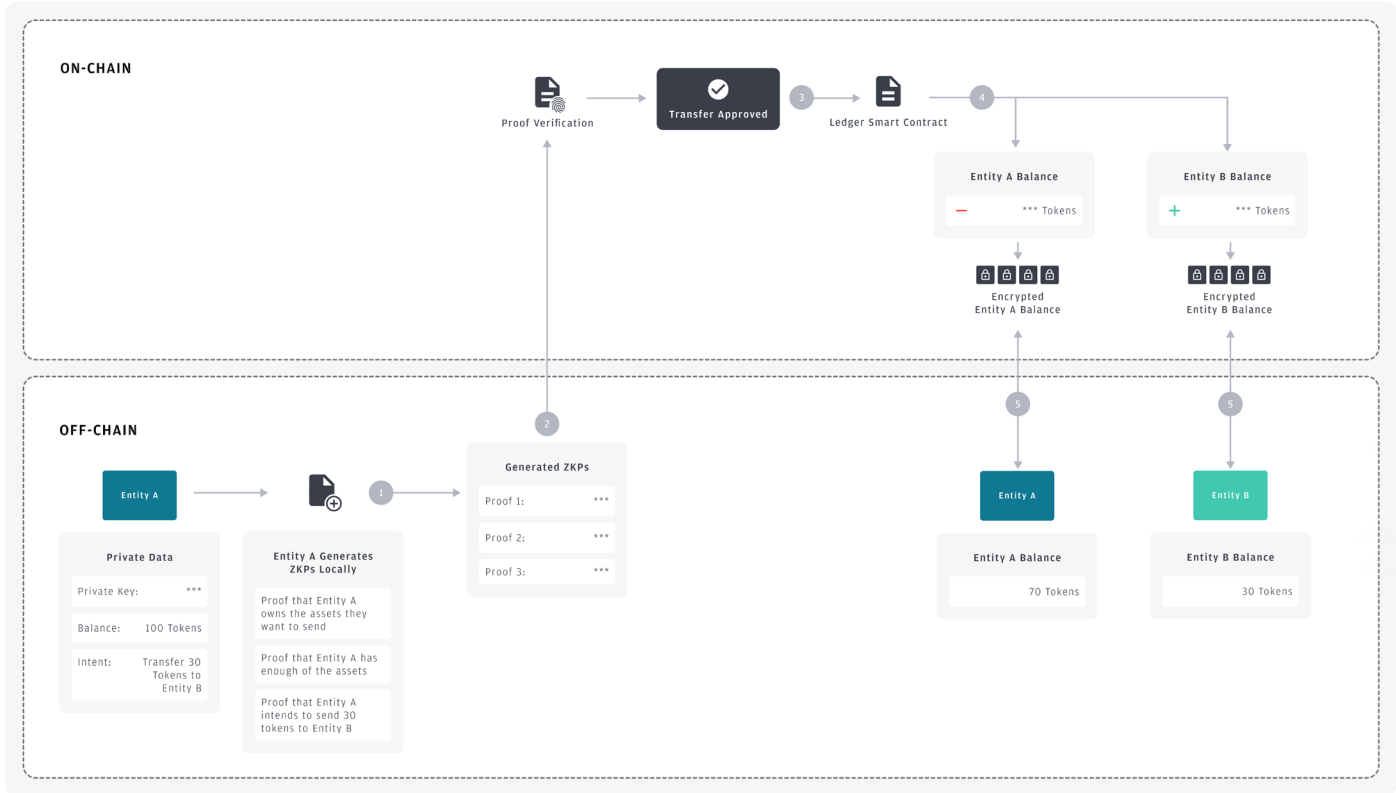
**Definition:** ZKPs are cryptographic methods that allow one party (the prover) to prove to another party (the verifier) that a statement is true without revealing any information beyond the statement's validity. ZKPs also allow provers to selectively reveal information about the original statement—for example, in response to a regulatory request for transaction information.

**Demystified:** Consider a simple illustration: proving knowledge of a padlock's combination. The prover demonstrates possession of the correct combination by unlocking the padlock outside the verifier's view, then presenting the opened lock. The verifier gains certainty that the prover knows the combination, without learning the combination itself.

### Use cases for ZKPs include:

- **Transactions:** Prove a transaction is valid without revealing details of the transaction.
- **Identity:** Prove your age without revealing any identity details.
- **Scalability:** ZK rollups are used to aggregate multiple transactions into a single proof which can be verified more easily.

# Zero-Knowledge Proofs (ZKP) Flow



## Walkthrough:

**Scenario:** Entity A wants to transfer on-chain assets to Entity B using a ZKP-based on-chain privacy ledger to achieve anonymity and confidentiality.

- 1 Entity A generates a transaction containing a number of ZKPs created from their private data:
  - A Proof that Entity A owns the assets they want to send
  - B Proof that Entity A has enough of the asset (in order to send it)
  - C Proof that Entity A intends to send to Entity B
- 2 Entity A sends the transaction to a verifier smart contract which validates the ZKPs without revealing the private data. The ZKP system ensures each transaction's correctness by proving that the transaction sender owns the assets they are trying to transfer, the asset hasn't previously been transferred, and that no assets would be created or destroyed during the transfer, all without revealing the private data.
- 3 Once the proof is validated, the verifier smart contract sends the encrypted outputs to the ledger smart contract.
- 4 The ledger smart contract updates its encrypted global state and stores the new encrypted balances on-chain.
- 5 Entity A and Entity B, using their own off-chain private data, are the only parties who can decrypt their new on-chain balances for tracking. Note: Entity A and Entity B will compute their respective aggregate balances off-chain.

## Stealth Addresses

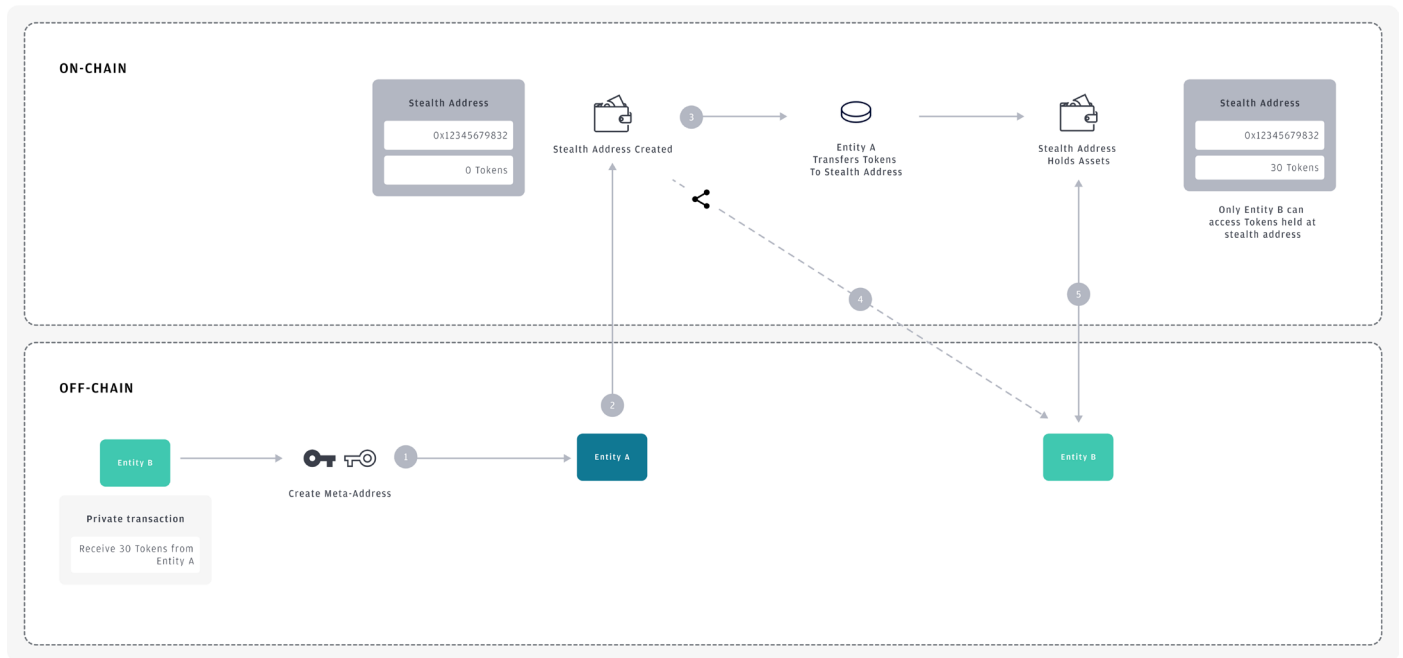
**Definition:** Stealth addresses, defined under (Ethereum Request for Comments) ERC-5564<sup>24</sup>, are an on-chain privacy technique that enables secure, private transactions through dynamic address generation. At its core, this technology uses smart contracts to allow a sender to create a new public address for a receiver without the sender being able to access the public address themselves. This enables receivers to use the funds in the newly created address without revealing their original on-chain address, thereby protecting their identity and transaction history.

**Demystified:** Consider an online mailbox system where each transaction generates a unique mailbox, accessible only to the intended recipient. The sender creates this mailbox but cannot access it themselves, ensuring complete privacy of the receiver's identity and transaction patterns.

### Use cases for stealth addresses include:

- **Privacy:** Receive payments without revealing your identity or transaction history.
- **Security:** Protect your public address from being linked to transactions.

## Stealth Address



### Walkthrough:

**Scenario:** Entity A wants to transfer on-chain assets to Entity B using stealth addresses to improve anonymity.

- 1 Entity B generates and shares a “meta-address” with Entity A. A meta-address is similar to a public address (e.g. Ethereum EOA) in that it is publicly shareable, however its distinct use of keys allows for the creation and use of stealth addresses.
- 2 Entity A uses Entity B’s meta-address to create a new unique address for the transaction. This ensures that the transaction is sent to an address not associated with the Entity B’s identity, or their previous transactions, hence the address is “stealth”.
- 3 Entity A transfers the on-chain assets, using standard methods (e.g. ERC-20 Transfer), to Entity B’s newly created stealth address (which has no prior transaction associated with it).
- 4 Entity B can listen for on-chain announcements to identify new stealth addresses intended for them.
- 5 Only Entity B’s meta-address private key can derive the private key to the new stealth address, and thus only Entity B can control the assets in the new stealth address.

# Fully Homomorphic Encryption

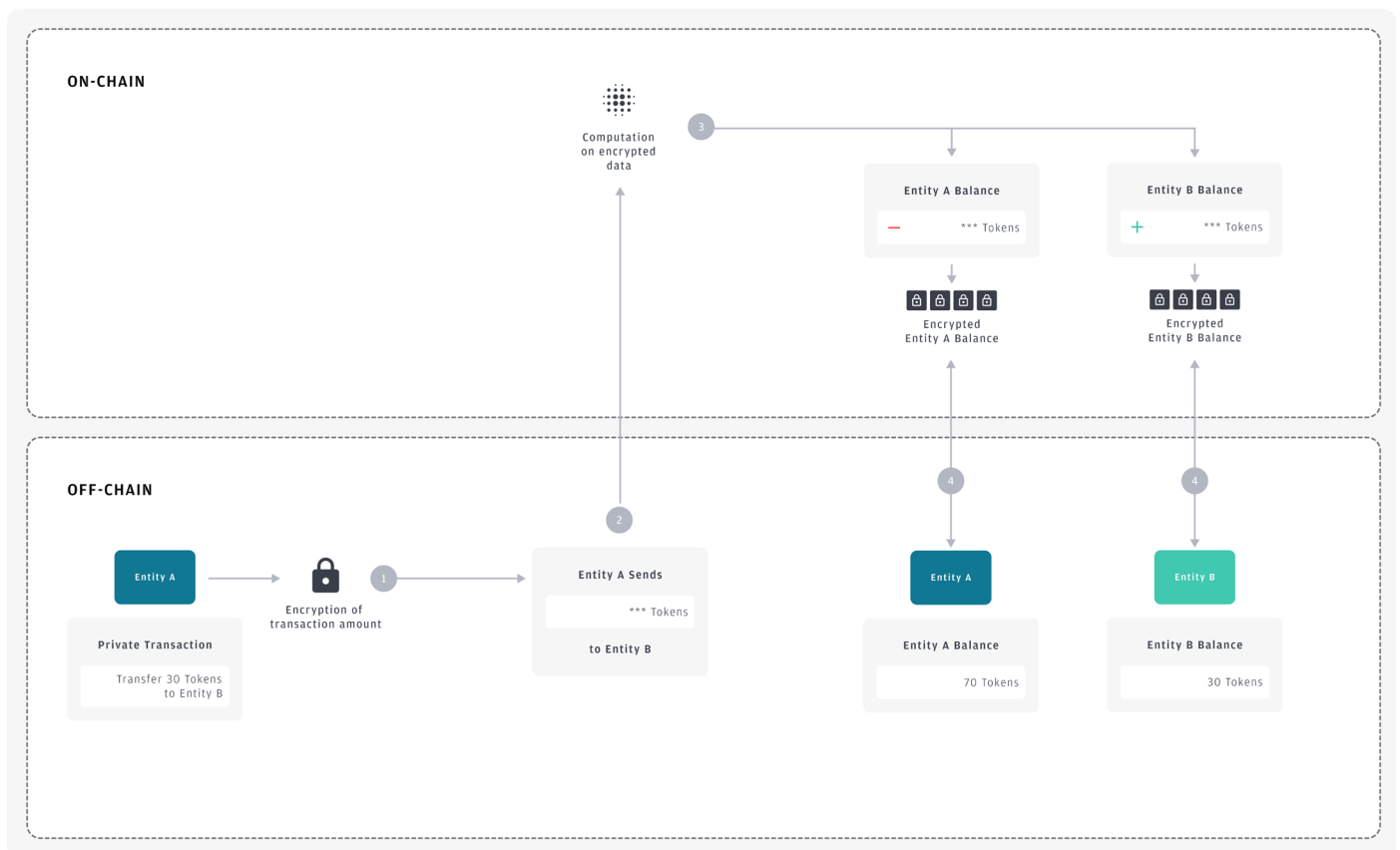
**Definition:** FHE is an encryption scheme that allows computations on encrypted data without decryption. The results remain encrypted and only the holder of the decryption key can access the unencrypted output.

**Demystified:** FHE allows users to do mathematical operations on private inputs and arrive at the correct output, without ever revealing the input or the output. Imagine a deconstructed 1,000-piece puzzle where each piece has an image, but the full picture is unknown. You want your friend to solve it without seeing the imagery on the puzzle pieces. You remove the images from the puzzle pieces (encryption) and give them to your friend. They assemble the puzzle by matching edges (computation) and return the completed, imageless puzzle. You then reapply the images to the puzzle pieces (decryption) and see the full picture.

## Use cases for FHE include:

- **Privacy:** Perform computations on sensitive data without exposing it.
- **Secure data analytics:** Analyze encrypted datasets without decrypting them.
- **Confidential machine learning:** Train and infer on encrypted data without revealing the underlying information.

## Fully Homomorphic Encryption (FHE) Flow





## Walkthrough:

**Scenario:** Entity A wants to transfer on-chain assets to Entity B using on-chain FHE to improve confidentiality.

- 1 Entity A locally encrypts the amount they want to transfer to Entity B and includes the encrypted amount as part of the transaction but otherwise submits the transaction on-chain through normal methods.
- 2 The transaction is broadcast to the blockchain. Since the amount being sent is encrypted, it remains shielded from external observers.
- 3 The on-chain FHE checks the validity of the transaction and then executes the transaction without decrypting the encrypted amount. Since FHE allows for on-chain computation, aggregate encrypted balances are updated on-chain.
- 4 Once the transaction is confirmed as valid and settled on-chain, Entity A and Entity B are able to use their private keys to decrypt their new balances.

## Privacy Features

Different solutions for enhancing privacy on the blockchain, both on-chain and off-chain, offer unique benefits and trade-offs. The radar charts below illustrate how various approaches perform across some of the key technical features essential for enterprise privacy on the blockchain.

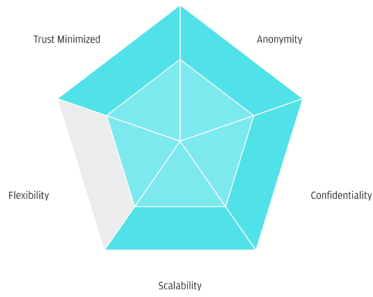
- **Anonymity:** The ability to shield the identities of the parties involved in a transaction from anyone outside of the transaction.
- **Confidentiality:** The ability to not shield the asset type and quantity being transacted from anyone outside of the transaction.
- **Scalability:** The ability of a system to handle an increased transaction rate or expand in capacity without performance degradation.
- **Flexibility:** The capability to program custom logic into the solution, on-chain.
- **Trust Minimization:** The reduction of the need to rely on third parties or intermediaries for security and correctness.

Each solution was assessed according to the criteria above for its level of effectiveness, where:

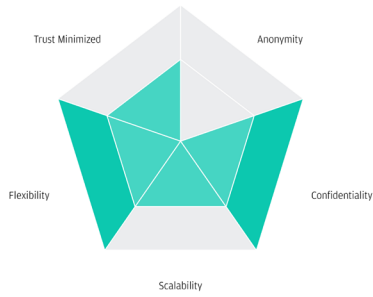
- A score of low indicates minimal effectiveness in the respective category.
- A score of medium signifies a medium level of effectiveness.
- A score of high represents a high level of effectiveness.

## Evaluating Privacy Solutions

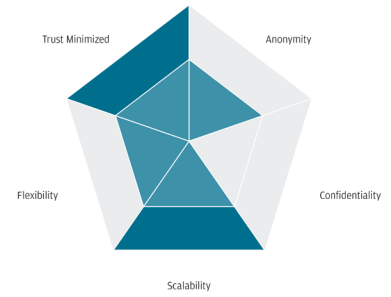
### ZERO-KNOWLEDGE PROOF (ZKP)



### FULLY HOMOMORPHIC ENCRYPTION (FHE)



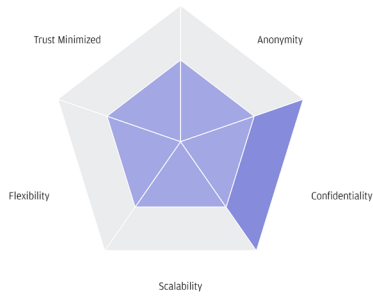
### STEALTH ADDRESSES



### CENTRALIZED ACCESS CONTROL



### SILOED DATA



### TRUSTED EXECUTION ENVIRONMENT (TEE)



#### LEGEND



High



Medium

Low

For illustrative purposes only, the ratings reflect Onyx's current understanding and assumptions based on available research and are subject to change as technologies evolve

# What is Digital Identity?

## Introduction to Digital Identity

Digital identity enables individuals and institutions to receive and hold attestations from various trusted entities. These attestations can be shared with third parties to verify specific facts, allowing users to prove not only “who they are” but also “what they do”. This capability facilitates a variety of use cases, such as participating in secondary trades, by streamlining the process of KYC compliance and regulatory requirements. Its significance lies in providing a secure, private and verifiable means to establish trust among financial entities, investors and third parties.

## 1 Verifiable Credentials and DIDs

**Definition:** Verifiable Credentials (VCs) are digital attestations issued by a trusted authority that confirm certain attributes about an individual or entity. These attestations can be shared as Verifiable Presentations (VPs), which package VCs in a tamper-proof format, linking them to the individual. They can be cryptographically verified to ensure authenticity and integrity. Decentralized Identifiers (DIDs) are unique identifiers created, owned and controlled by the individual, offering greater privacy and control over digital identity. DID registries and trust registries are part of governance frameworks that manage the issuance, revocation, and verification of DIDs and VCs, ensuring compliance with standards and protocols.

**Example:** A transfer agent could issue AML/KYC attestations to investors, enabling them to access and share their credentials directly from their digital wallets. Each investor could be identified by a unique Decentralized Identifier (DID), linking all attestations seamlessly. This integration of DIDs, Verifiable Credentials (VCs), and Verifiable Presentations (VPs) helps to ensure that AML/KYC attestations are portable, trackable, and revocable, enhancing compliance and operational efficiency.

## 2 Soulbound tokens (SBTs)

**Definition:** Soulbound tokens are non-transferable tokens that represent unique attestations tied to an individual's digital identity. They establish a persistent and verifiable record of certain characteristics or achievements.

**Example:** Transfer agents could issue AML/KYC attestations in the form of soulbound tokens to investors' wallets. These tokens could be permanently linked to the investor's wallet, providing a seamless verification process. When investors connect to financial platforms, verifiers could instantly confirm the presence of an AML/KYC soulbound token, streamlining compliance checks.

## 3 Non-Fungible Tokens (NFTs)

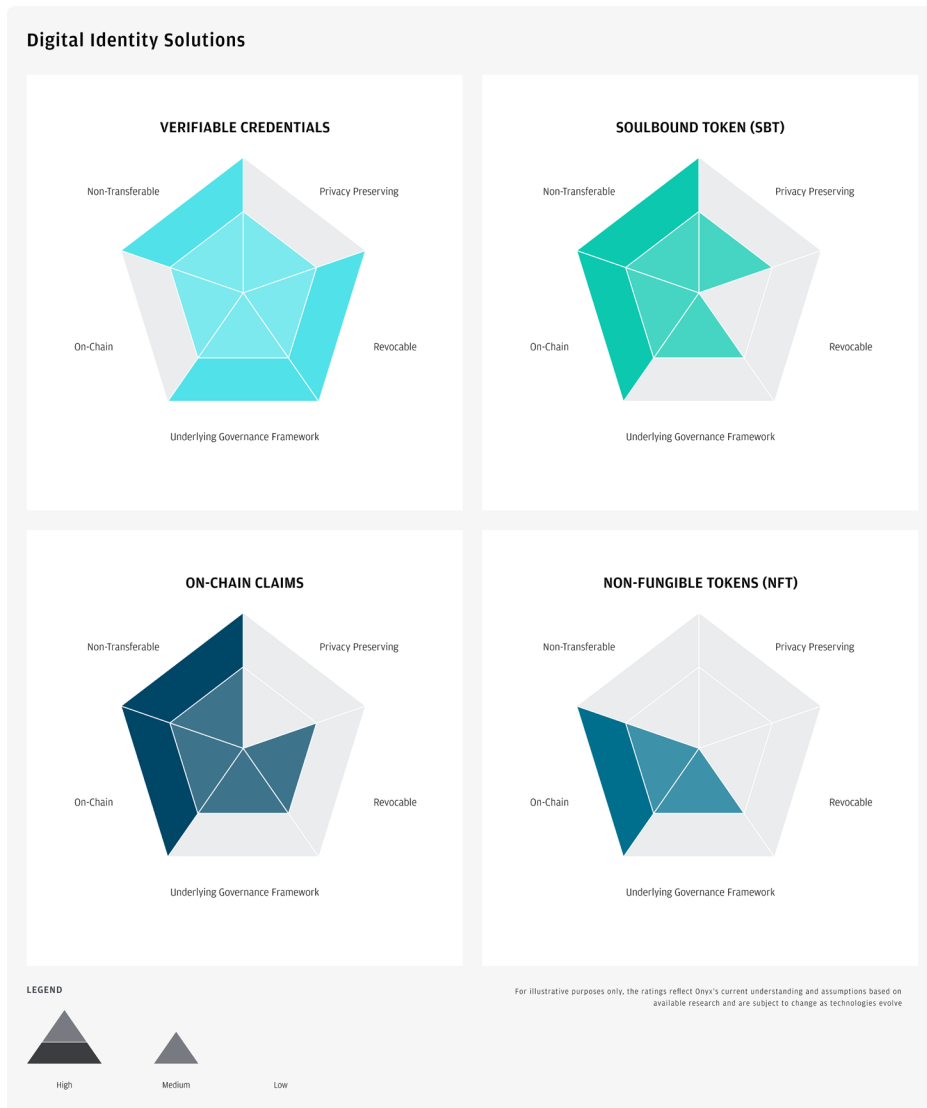
**Definition:** NFTs are unique digital assets that represent ownership or proof of authenticity for various items, including digital identity attestations. They allow for the tokenization and trading of unique identity-related information.

**Example:** Transfer agents could issue AML/KYC attestations in the form of an NFT to investors' wallets. This approach allows financial platforms to quickly verify whether an investor holds the necessary AML/KYC NFT, ensuring compliance and enhancing the onboarding process.

## 4 On-chain Claims

**Definition:** On-chain claims are identity attestations stored and managed on a blockchain. They provide a secure and immutable record of identity-related information—accessible and verifiable by authorized parties.

**Example:** Transfer agents could store AML/KYC attestations on-chain, associating them with investors' public addresses. This setup functions as a dynamic ledger, linking attestations to wallets.



## Applicability of Privacy to On-Chain Identity

The concept of on-chain privacy, as previously discussed, should encompass confidentiality, anonymity and auditability. Technologies like ZKP and encrypted on-chain claims, such as FHE, can facilitate creation of an on-chain identity framework that preserves privacy.

## 5 Identity ZKPs

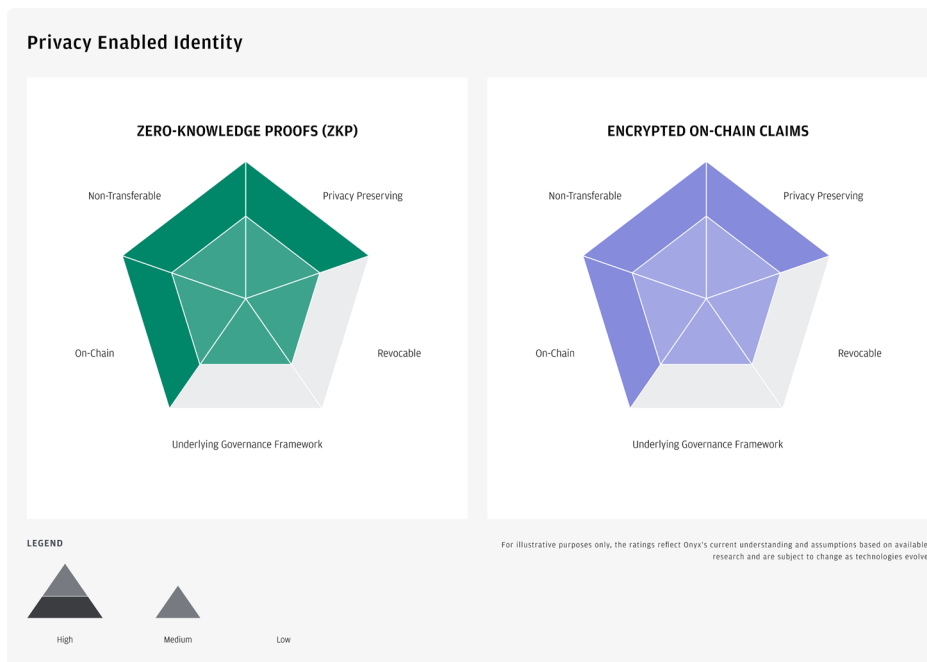
**Definition:** As previously defined, ZKPs are cryptographic techniques that allow one party to prove validity of information to another party without sharing the full underlying identity information. It is important to emphasize that ZKPs can be derived from various data sources. These include off-chain data, claims associated with a verifiable credential, and even evidence of the credential's existence.

**Example:** ZKPs enable investors to present proofs of their AML/KYC VCs to verifiers, such as other transfer agents, without sharing the underlying issued credential.

## 6 FHE - On-chain Claims

**Definition:** As previously defined, FHE is a fully Homomorphic Encryption (FHE) is an encryption scheme that facilitates the verification of on-chain attestations without the need for decryption. FHE can be used to encrypt on-chain identity attestations, enabling verifiers to assess specific criteria against these attestations while maintaining the confidentiality of their unencrypted values.

**Example:** Transfer agents typically have their own rules and identity requirements that investors must meet before being onboarded to a fund. This may include AML/KYC attestation and on-chain sanction lists. These attestations can be encrypted on-chain, allowing transfer agents to verify the identity requirements against their rules without needing to view the underlying data



# Building Ecosystem Trust and Ensuring On-Chain Privacy for Identity

Each identity and privacy technology has its own capabilities and can be applied to different use cases based on specific requirements. For this project, we focused on two key themes that are crucial: ecosystem trust and on-chain privacy.

The ecosystem of participation and trust extends beyond technical solutions, emphasizing the importance of establishing trust among participants, such as transfer agents, fund administrators and other financial institutions. Without this trust, any identity or privacy technology will face headwinds in achieving widespread adoption, regardless of its robustness or sophistication.

On-chain privacy is primarily concerned with the ability to maintain AML/KYC identity claims on public blockchain without revealing any PII. Ensuring on-chain privacy is essential for protecting individual identities, while still allowing the necessary verification processes for expedited investor onboarding.

## 1 Verifiable Credentials and DIDs

- **Governance Framework:** Digital identity extends beyond a technical challenge; it requires a cohesive business approach. Transfer agents and market participants must align around a unified set of infrastructure solutions. By adopting frameworks like W3C Verifiable Credentials (VC) and Decentralized Identifiers (DID), agreed-upon, trusted issuers and standardized schemas—such as for AML letters—can be established, fostering mutual understanding and trust across the ecosystem.
- **Revocability:** The evolving regulatory landscape and investor dynamics demand the ability to revoke, and update, identity credentials. This capability is essential for maintaining accurate and reliable identity information, particularly as transfer agents navigate changing regulations and ongoing monitoring.
- **Non-Transferability:** The need for identity credentials to remain uniquely tied to individuals is crucial for preventing misuse and maintaining the integrity of the verification process. Digital identity facilitates a world of portable, reusable credentials without compromising their integrity.

## 2 Enabling On-Chain, Privacy-Preserving Identity

- **On-Chain Compatibility:** As tokenized cash and assets flow on public blockchains, identity must operate natively on-chain. While some funds and transfer agents currently perform AML/KYC checks off-chain, achieving full programmability and integration requires both identity checks and tokenized assets to function harmoniously on-chain.

- **On-Chain Privacy Preservation of Identity:** Privacy concerns are vital in public blockchain networks, especially for financial institutions. In a future state where identity is on-chain, preserving privacy is crucial. Pii must remain confidential. Technologies like ZKPs and FHE can address these concerns by enabling verification without exposing sensitive data, ensuring regulatory compliance and data protection.

The radial diagrams illustrate that solutions like Verifiable Credentials and their associated trust frameworks effectively fulfill the criteria for achieving ecosystem trust. Conversely, technologies such as ZKP and Fully Homomorphic Encryption (FHE) effectively meet the criteria for ensuring privacy-preserving identity.

Based on the above assessment, the optimal strategy for meeting all five criteria involves integrating digital identity solutions with privacy-preserving technologies.

# Requirements and Evaluation: Defining the use cases

To compare solutions for privacy, identity, and composability in tokenized funds, we selected three key use cases, outlined business and technical requirements, and invited technology platforms in the privacy space to implement these requirements as a technical proof of concept.

These flows and requirements are summarized below. Individual case studies pertaining to each implementation can be found in the Appendix.

	Use Case	Example
1	<p>Ensure Delivery vs. Payment (DvP) settlement of transactions can occur privately:</p> <ul style="list-style-type: none"><li>✓ Confidentiality of transaction amount</li><li>✓ Confidentiality of transaction type</li><li>✓ Confidentiality of token type</li><li>✓ Anonymity of investor addresses</li></ul>	<p>An institutional investor is able to subscribe into a fund, but their identity, the fund being entered, and the amount being invested remains private.</p>
2	<p>Ease the onboarding process of investors through reusable AML / KYC and enable automation by using privacy-preserving on-chain identity claims:</p> <ul style="list-style-type: none"><li>✓ Preserve the privacy of identity attributes</li><li>✓ Deploy reusable on-chain identity verification</li></ul>	<p>An institutional investor is able to verify their information once at the point of onboarding where a verifiable credential is issued. Following that, at any additional points in the lifecycle where the institutional investor's identity needs to be verified, privacy-preserving identity claims can be added and checked on-chain to simplify the process.</p>
3	<p>Demonstrate new use cases can be built atop private assets and private identity infrastructure:</p> <ul style="list-style-type: none"><li>✓ Preserve composability</li><li>✓ Drive asset utility</li><li>✓ Automate compliance checks on AML KYC attestations</li><li>✓ Re-use identity infrastructure</li></ul>	<p>An institutional investor is able to take fund units they own and privately sell them on the secondary market to a buyer whose AML/KYC status has been pre-verified.</p>



# End-to-End Workflow

- A fund manager establishes funds for tokenization by a transfer agent on a blockchain network.
- Investors who have a verified identity can subscribe into available fund using on-chain cash balances.
- An investor's identity and investment ability is validated through a digital identity solution according to a transfer agent's standards.
- A separate application/utility - for secondary markets - allows investors to transact (buy/sell) fund units with other verified investors.

All while maintaining transaction privacy, identity privacy and composability.

Across the workflow, we also tested for:

## Business Requirements:







- **Selective Disclosures:** Mechanisms that would allow certain parties to receive authorized access to view specific attributes of private information (e.g. an auditor or regulator).
- **Atomic Delivery vs. Payment (DvP):** Simultaneous delivery and payment for assets within a block<sup>25</sup> –the core element that reduces settlement risk.
- **Block Explorer:** Validation through a block explorer to transparently demonstrate privacy features.

## Technical Requirements:

- **Open-Sourced Solution:** Understand which open-source libraries have been utilized in the implementation.
- **Trust-Minimization:** Determine the solution's ability to operate within a fully decentralized network of peers, and its reliance on security mechanisms, such as Key Management Services.
- **Similarity to Development on EVM:** Determine the extent of necessary changes to standard Solidity<sup>26</sup> smart contracts (e.g. ERC-20; KDA-FACT; etc.) to integrate with the privacy solution.
- **Identity Handling:** Examine flexibility in handling on-chain and off-chain identity, including support for claims, proofs, encrypted verifiable credentials, and decentralized identifiers.
- **Performance:** We acknowledge that performance metrics are critical for production usage, however standardizing all technical variables was infeasible across varying implementation and infrastructure in the given timelines. The evaluation focused on feasibility as opposed to optimization.

# Findings

The technology providers we selected represent a handful of EVM compatible privacy solutions with unique approaches to ZKPs, FHE, and stealth addresses. For the digital identity component the technical contributors explored both in-house and open-source implementations. Dummy assets, actors, and identities were used throughout each use case.

	 				
<b>Overview of Privacy Provider</b>	Kinexys used Zama's open-source fhEVM-native solution to keep balances and transaction amounts encrypted, ensuring confidentiality while maintaining composability through FHE.	PADL, developed by JPMC's Global Technology Applied Research team, leverages ZKPs for on-chain verification, ensuring confidentiality and anonymity by hiding transaction details and identities, while maintaining auditability.	Avacy anonymizes user identities and obfuscates balances and transaction amounts using Distributed Homomorphic Encryption (DHE), stealth addresses, and ZKPs (zk-SNARKs), while enabling auditability.	Rayls' Private Subnets use segregated Privacy Ledgers (PLs) run by each institution, connecting via a permissioned EVM network called a 'Commit Chain'. Transactions are encrypted and posted to the Commit Chain, and validated with cryptographic inclusion proofs.	Fhenix is an Ethereum Layer-2 solution that enhances privacy by utilizing FHE to perform computations on encrypted data, such as balances and transaction amounts.
<b>Privacy technology used</b>	FHE, Stealth Addresses	ZKP	ZKP, Distributed Homomorphic Encryption (DHE), and Stealth Addresses	Segregated ledgers, cryptographic inclusion proofs, and encrypted point-to-point messaging	FHE
<b>Confidential Ownership Balance</b>	✓	✓	✓	✓	✓
<b>Confidential Transaction Value</b>	✓	✓	✓	✓	✓
<b>Confidential Transaction Type</b>	✗	✓	✓	✓	✗
<b>Confidential Token Type</b>	✗	✓	✗	✓	✗
<b>Confidential Bids</b>	✓	✓	✓	✓	✗

The information in this report, or on which this report is based, has been obtained from sources that the authors and/or J.P. Morgan believe to be reliable and accurate. However, such information has not been independently verified, and no representation nor warranty, express or implied, is made as to the accuracy or completeness of any information obtained from third parties.

<b>Anonymity of User Addresses</b>	✓	✓	✓	✓	✗
<b>Confidential Smart Contract logic</b>	✗	✗	✗	✓ In PL ✗ On Commit Chain	✗
<b>Identity Features Enabled</b>	DIDs, VCs, Encrypted on-chain claims	ZKP	DIDs, Encrypted on-chain claims, ZKP, Separate Compliance Chain	Ethereum Attestation Service	Encrypted on chain claims in an NFT
<b>Provision of KYC/AML Attestation</b>	✓	✗ but could use same method as sanction check	✓	✓	✓
<b>Verification of KYC/AML Attestation</b>	✓	✗ but could use same method as sanction check	✓	✓	✓
<b>Sanctions check</b>	✓	✓	✗ but could use same method as KYC/AML check	✗ but could use same method as KYC/AML check	✗ but could use same method as KYC/AML check
<b>1. What attributes can be included in credentials/identity system?</b>	1. Any attributes can be incorporated provided it can be represented by encrypted data types.	1. Any attribute can be included.	1. Any attribute can be included.	1. Any attribute can be included.	1. Any attributes can be incorporated provided it can be represented by encrypted data types.
<b>2. What attributes were actually used in verification &amp; sanctions checking process, where were they stored, and how were they checked?</b>	2. Two variable claims were utilized: an AML Letter with a true/false value and a Country Code, both encrypted using FHE and kept on chain in a smart contract. We also included the issuer of the original VC, from which these claims are derived, along with the VP hash. These claims were then homomorphically checked by the specified asset rules.	2. In the implementation, several representative rules were encrypted into a token and verifiable by any auditor.	2. In the implementation, identity credentials consist of encrypted name, surname, government ID, birth date, phone, and country of residence, which reside in a smart contract on the main chain and can be homomorphically checked or relayed to the compliance chain to decrypt and send back a Boolean result.	2. The attribute that was checked in the implementation was the 'suitability' attribute determined by the bank issuing the credential on its PL. All identifiers are kept off-chain and only the attestations are in the PL; the merkle root is shared through encrypted messages to a destination PL over the Commit Chain which can then decrypt the message and check the inclusion proof.	2. In the implementation, a KYC check was done with ID, name, and phone number attributes which were kept encrypted on-chain in an NFT and could then be homomorphically checked.
<b>Auditability</b>	The network's KMS operator would need to provision the auditor with the FHE decryption key to review all transactions. The trusted stealth address service could also specify addresses that are allowed to decrypt transactions.	3 different ways to do so: 1. Use ZKP for specific questions. 2. Specify parties to decrypt transactions with audit signatures. 3. Perform a full audit by decrypting and sharing results using ZKP for validation.	The ZK system requires users to encrypt transaction summaries with public visibility keys. Entities managing the application own the corresponding private keys, which can be shared with auditors.	Not implemented in POC but can use the 'God View' functionality which would allow any auditor to access details of any transaction by a PL.	Utilizes on-chain permissions contract which can specify parties that can decrypt.

The information in this report, or on which this report is based, has been obtained from sources that the authors and/or J.P. Morgan believe to be reliable and accurate. However, such information has not been independently verified, and no representation nor warranty, express or implied, is made as to the accuracy or completeness of any information obtained from third parties.

**Technical Uplift From EVM**

Requires slight modifications of ERC-20 contract to incorporate encrypted data types. Modifications / precompiles required on the EVM to enable FHE.

Extended functionality to implement PADL EVM-compatible ERC-20 smart contract for privacy preserving functions.

Supports ERC-20 and need to extend functionality to work with Avacy and deploy precompiles for DHE to ensure arbitrary confidential smart contracts are possible.

Deploy ERC-20 contracts as is in own PLs, but must extend functionality to work with Rayls Protocol, as well as register the token contract byte code to the Commit Chain.

Requires slight modifications of ERC-20 contract to incorporate encrypted data types and homomorphic encryption functionality. Modifications / precompiles required on the EVM to enable FHE.

**Composability**

Interact with assets similarly to ERC-20 tokens, enhanced by Zama's encryption functions. Asset contracts link to rules requiring on-chain identity verification. This solution allows reusable encrypted claims for smart contracts to specify their required claims.

Interact with assets with ERC20 like functions on the PADL contract and can extend a PADL contract to support additional functionality.

Must generate ZKPs to reference the asset smart contract, if approved, provide a ZKP for identity checks as specified by the asset contract and verified on the compliance chain. In order to interact with an asset, to maintain privacy in own contract, builders must create their own ZKP circuits or use DHE.

To interact with an asset in a separate PL, a user's identity is checked and asset balance updated through Rayls Protocol which manages cross-chain messaging and cryptographic proofs of inclusion via the Commit Chain.

Assets interaction is similar to ERC-20 tokens, enhanced by Fhenix's encryption functions. Assets specify an NFT contract for attribute verification, requiring users to verify their identity and add their address to the NFT contract to interact with the asset.

**Centralization Points**

- Centralized KMS
- Trusted Stealth Address Service
- Trusted Verifier Service

The system is not centralized by design, however the auction flow has a trusted operator actor in the current implementation.

- Application owners' visibility keys (if they are set)
- Trusted KYC service
- DHE permissioned key sharing amongst validators

- PL - centralized actor that custodies their users' keys
- Subnet Operator - sets up the network and oversees its governance
- Auditor - uses a 'God View' and 'Flagger' feature to listen to all transactions and send signals when a PL is acting dishonestly

- Threshold KMS with trusted actors
- Trusted KYC service

The information in this report, or on which this report is based, has been obtained from sources that the authors and/or J.P. Morgan believe to be reliable and accurate. However, such information has not been independently verified, and no representation nor warranty, express or implied, is made as to the accuracy or completeness of any information obtained from third parties.

# Privacy: Reflection on the Outcome

## Technology

## Why Is This Interesting?

## Challenges

### Zero-Knowledge Proofs (ZKPs)

ZKPs are particularly compelling for fund tokenization as they enable critical verifications while maintaining confidentiality. Fund managers can validate investor eligibility, process transactions, and meet compliance requirements, without exposing sensitive data. The technology is already in use in live blockchain environments and can be implemented without fundamental changes to existing infrastructure, making it a practical choice for institutional adoption.

#### Core Capabilities:

- Addresses anonymity and confidentiality
- Enables transactions without revealing information
- Enables flexible and programable auditability

#### Technical Benefits:

- Scalable, effective anonymity and composability
- Usable on-chain without blockchain modification

#### Implementation Advantages:

- Widely used in live blockchains
- ZK Domain Specific Languages (DSLs<sup>27</sup>) accessible
- Effective relayer services, or stealth addresses, for anonymizing transactions

While technically viable, implementing ZKPs requires adapting current fund processes and standards. The computational requirements, though manageable for institutions, need consideration when designing systems. The lack of established industry-wide cryptographic standards means early adopters will need to carefully plan their implementation approach.

#### Technical Challenges:

- Smart contract standards differ from current institutional techniques
- Requires client-side computing power. Although the blockchain community has driven significant improvement

#### Implementation Hurdles:

- Computational requirements remain substantial
- Decentralization needed for transaction submission service, if used

#### Current State Limitations:

- Cryptographic standards not established
- Path to industrializing ZK unclear

### Stealth Addresses

Stealth addresses offer a straightforward and effective solution for transaction privacy in fund operations. They enable confidential fund interactions—from subscriptions to distributions—without exposing investor relationships or transaction patterns. The technology's simplicity and compatibility with existing systems makes it particularly attractive for near-term implementation.

#### Core Capabilities:

- Scales well in practice
- Provides anonymity for single transactions
- Simple to implement

#### Technical Benefits:

- Achieves anonymity levels not available in FHE EVMs
- Used for anonymous smart contract transactions

#### Implementation Advantages:

- Manages identity linkage without breaking anonymity
- Requires no changes to the EVM

The primary hurdle is the cost structure on public blockchains, where generating new addresses for frequent fund transactions could become expensive. While this has been solved in some implementations through gasless blockchains, institutions need to carefully consider the cost implications for their specific use cases.

#### Technical Challenges:

- Gas requirements on public blockchains can link back to owner

#### Implementation Note:

- Used in a gasless blockchain to eliminate gas-related challenges

## Technology

## Why Is This Interesting?

## Challenges

### Fully Homomorphic Encryption (FHE)

FHE presents the possibility of performing crucial fund calculations and processes while maintaining complete data privacy. It could enable confidential NAV calculations, portfolio management, and regulatory reporting, while keeping sensitive information encrypted throughout. The ability to upgrade existing smart contracts to incorporate FHE makes it an interesting option for enhancing current systems.

#### Core Capabilities:

- Keeps sensitive data encrypted throughout computation

#### Technical Benefits:

- Existing smart contracts can be upgraded to use FHE
- Clear applications outside of blockchain

The new technology sees significant practical hurdles in its current state. It requires modifications to blockchain infrastructure, faces scalability challenges, and introduces complexity that could impact time-sensitive fund operations. While solutions exist for some challenges, they often involve trade-offs between efficiency and centralization. The technology's maturity level suggests it may be better suited for longer-term implementation planning rather than immediate deployment.

#### Technical Challenges:

- EVM modification required for on-chain implementation
- Computational complexity impacts scalability and gas fees

#### Implementation Note:

- Off-chain processing improves scalability but introduces centralization
- Development challenging due to evolving capabilities
- Compressed FHE calculations require some centralization

#### Current State Limitations:

- Solutions maturing for on-chain usage
- Maturity needed for on-chain implementation

## Summary

Privacy technologies present varying degrees of maturity and applicability for institutional adoption.

ZKPs demonstrate the most comprehensive capability for meeting privacy requirements, though their implementation necessitates significant shifts in development approach and integration patterns. The emergence of standardized frameworks for ZKP implementation in smart contract privacy pools signals growing industry maturity.

While FHE alone cannot fully address institutional privacy needs, its combination with ZKPs and/or stealth addresses creates a more complete privacy solution. FHE's unique ability to process encrypted data offers promising innovation potential, though its required modifications at the EVM level may complicate future blockchain upgrades.

Stealth addresses represent an elegant, scalable solution that shows promise beyond current applications. Their simplicity and effectiveness make them particularly attractive for specific use cases.

The optimal approach to achieving comprehensive on-chain privacy will ultimately depend on specific use cases and requirements. Implementation decisions must consider the characteristics of the target blockchain – for instance, gas fees on certain networks may make computationally intensive operations impractical.

As these technologies evolve, continued evaluation and adaptation will be crucial for maximizing their potential in institutional applications.

# Conclusion and Future Outlook

## **1 Enterprise privacy, identity and composability on-chain will fuel tokenized finance.**

While initial asset tokenization efforts can progress without comprehensive privacy and integrated identity solutions, scaling institutional adoption requires both. The transformation of traditional finance through tokenization depends on meeting these fundamental requirements.

## **2 On-chain cryptographic blockchain privacy solutions promise stronger guarantees and openness than traditional off-chain (segregation based) privacy approaches, yet must balance sophistication with pragmatic deployment needs for adoption.**

EVM blockchain ecosystems offer innovative privacy solutions through ZKPs, FHE and stealth addresses, integrating directly with the blockchain rather than relying on off-chain data segregation and access controls. While this native integration provides robust confidentiality guarantees and eliminates compromise points, the path to institutional adoption requires careful consideration of implementation challenges. The optimal solution varies by use case – some applications may demand a multi-faceted approach combining multiple technologies, while others might achieve their objectives through a single solution.

Current implementations demonstrate that on-chain privacy is achievable and performs adequately at modest scale. However, institutional adoption requires deeper exploration and validation across several critical dimensions: intensive computational requirements, fundamental infrastructure adaptations, network cost considerations and lack of standardized integration patterns. Advancing these solutions demands focused development in processing optimization, resource efficiency and comprehensive developer frameworks suitable for institutional-scale deployment.

## **3 Reusable digital identity promises operational transformation, however its implementation must be commercially viable i.e., it must align with established trust frameworks and create compelling participation incentives for adoption.**

Privacy-preserving, reusable digital identity solutions are fundamental to unlocking tokenization's full potential, enabling streamlined onboarding, real-time verification, and programmable compliance. However, successful implementation requires evolution beyond technical capability alone. Solutions must bridge traditional trust mechanisms – such as today's reliance letters between regulated entities – with new digital frameworks that incentivize participation across the ecosystem. This demands building a network of trusted institutions, from transfer agents to fund managers, where identity verification becomes a valuable service with clear economic benefits for providers.

Success requires several critical dimensions: scalable performance that meets institutional demands, seamless integration with existing trust frameworks while maintaining security standards, sustainable economics that incentivize adoption, and robust governance that establishes trust between market participants. The path forward requires not just technological sophistication, but thoughtful design of incentive structures that encourage institutions to participate in, trust, and leverage these digital identity networks.

## Call to action

**Engage:** We welcome dialogue from companies & projects exploring solutions for institutional-grade privacy and streamlined digital identity management. In addition to exploring the technology, we are focused on furthering industry alignment across standards & governance. Please reach out to us at [KDA\\_Growth@jpmorgan.com](mailto:KDA_Growth@jpmorgan.com).

**Build:** We are continuing on the journey of expanding access to our network - Kinexys Digital Assets - and our digital identity capabilities. Come with us on this journey.

Check out our Kinexys Self Sovereign Identity (SSI) SDK which enables the creation and management of decentralized identifiers (DIDs) and verifiable credentials (VCs). It supports integration into end-to-end SSI ecosystems, adhering to W3C standards and offers tools for creating custom schemas.

**Stay tuned.** Watch this page: We're committed to discovering and implementing privacy & identity solutions across the Kinexys Digital Assets suite. As we progress our thinking and collaborate with the ecosystem, we'll leverage this site to provide updates for the public.



# Appendix: Case Studies



## Kinexys by J.P. Morgan's implementation leveraging Zama's privacy solution

We deployed Zama's native fhEVM<sup>28</sup> solution within an Kinexys Digital Assets sandbox to execute the use case, maintaining on-chain privacy and identity while building utility with composable assets. Our implementation was composed of 3 key layers:

- 1 KDA fhEVM network:** We used Zama's native fhEVM solution to ensure that balances and transaction values are kept encrypted on the network. This set the foundation for the rest of our solution.
- 2 Stealth addresses:** An off-chain stealth address service, a modification to ERC-5564, provided anonymity by obfuscating the main addresses of each party in a transaction.
- 3 Digital identity:** We utilized our open-source Kinexys SSI SDK alongside FHE privacy technologies to develop a digital identity solution tailored to the business requirements of this proof-of-concept. This solution enabled encrypted investor identity claims to be programmatically verified on-chain, meeting automating AML/KYC checks performed by transfer agents and fund managers.

Together, the KDA fhEVM network, stealth addresses and digital identity solution enabled confidential, anonymous, compliant fund subscriptions and transfers across a global shared state network.

## Implementation overview

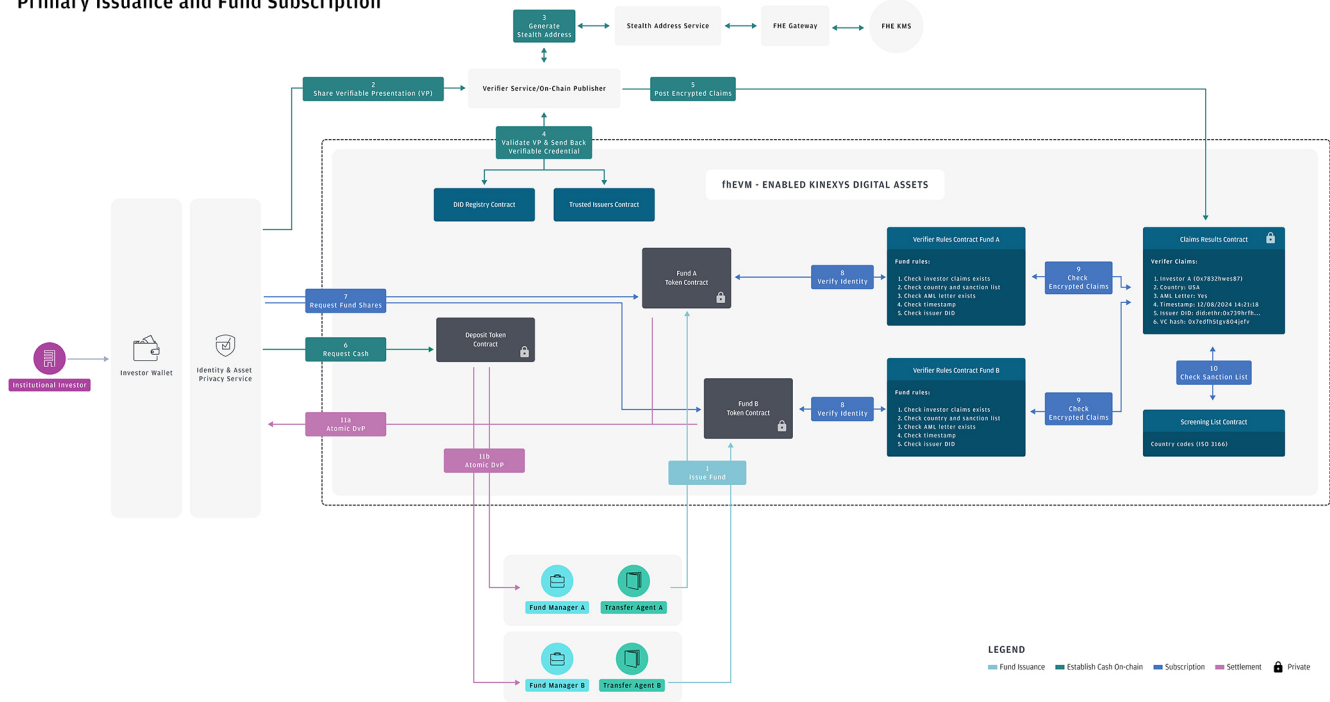
### Set Up and Deployment

Operators began by deploying the contracts onto the fhEVM-enabled KDA network - the unencrypted decentralized identifier (DID) registry contract and unencrypted trusted issuers contract were used as trust anchors for the issuance of verifiable credentials (VC). The transfer agents, as trusted entities, issued off-chain VCs to the institutional investors after performing necessary identity verification and AML checks. The VCs mirrored the structure of an AML letter, with additional data points and intrinsic characteristics of VCs. The institutional investors then stored and managed their credentials in their wallets for reuse.

A bank deployed an encrypted deposit token contract to enable the transfer of cash from off-chain to on-chain - where deposit tokens would be issued to the address requesting a balance.

## Primary Issuance and Fund Subscription

Primary Issuance and Fund Subscription



Two transfer agents deployed encrypted fund tokens on behalf of two respective fund managers on the fhEVM KDA network, making both available for subscriptions.

An institutional investor requested \$10M of deposit tokens, prompting the creation of a stealth address to ensure their original on-chain address is not linked to their new address receiving tokens. An off-chain verifier service was used to verify the institutional investor's VC and subsequently encrypt specific claims from the VC and map them to the stealth address in a smart contract on-chain. An off-chain verifier service was used to verify the institutional investor's VC and subsequently encrypt specific claims from the VC and map them to the stealth address in a smart contract on-chain. When received, the tokens are stored in an encrypted form.

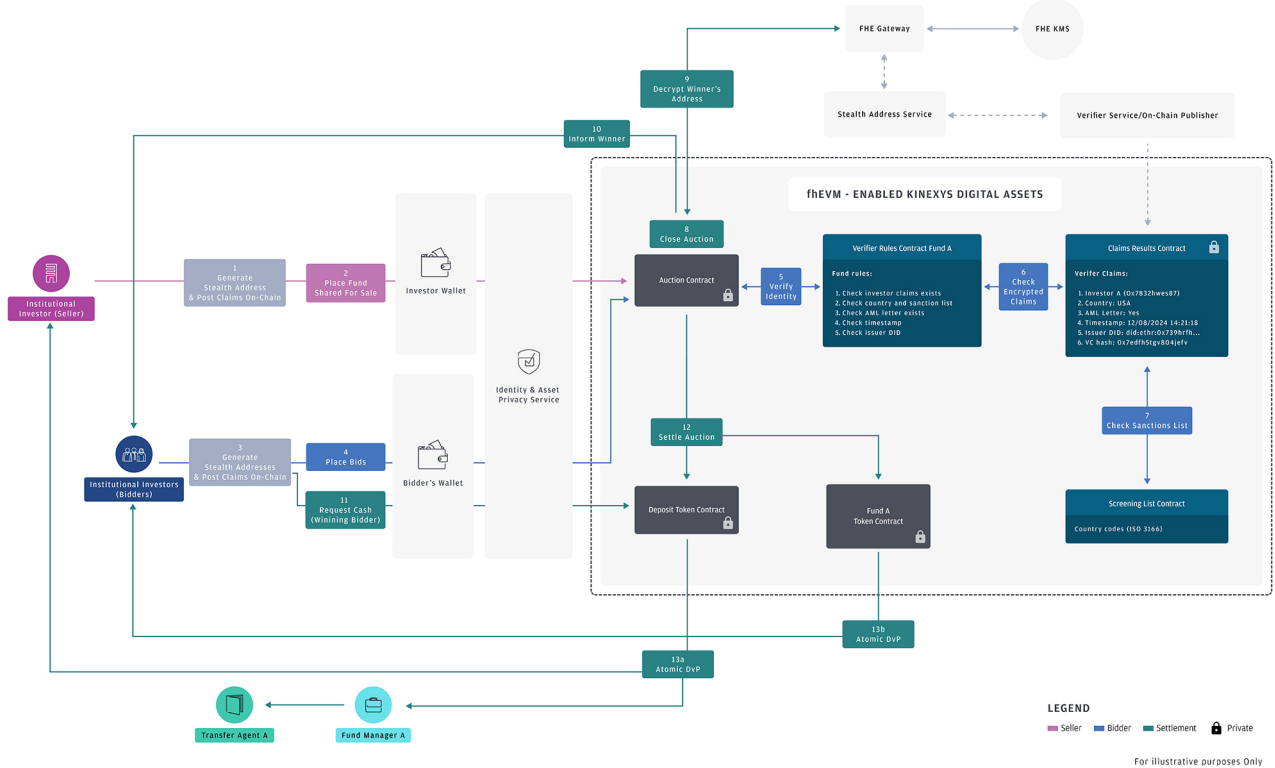
From this stealth address, the investor subscribed an encrypted \$5M of fund tokens into each fund, preapproving the transfer of their encrypted deposit tokens to the funds. Both fund contracts call for an identity check to perform on-chain verification of the investors encrypted claims. On-chain verification ensured that an investor was in compliance with AML/KYC fund rules and not on the sanctions list - all the while, keeping their claims encrypted

and private due to FHE.

Upon successful identity verification, atomic delivery vs. payment (DvP) completed, the investor received \$5M in encrypted fund tokens of each fund to their stealth address. Both fund managers received \$5M in encrypted deposit tokens each for the investor's subscriptions into the funds.

## Secondary Market Trading

### Secondary Market



The investor then decided to sell \$5M of their Fund A tokens on the secondary market, which prompted the creation of a new stealth address to ensure their identity is kept private. Using this new stealth address, the investor listed their Fund A tokens for auction at the encrypted auction contract - where the highest bid wins.

Other institutional investors on the secondary market wished to bid on the fund up for sale which prompted the creation of stealth addresses for each institutional investor bidding to ensure their identity was kept private.

When inputting interest to bid, each institutional investor prompted the generation of a stealth address for anonymity - following the same process as the prior flow. Each institutional investor submitted their encrypted bids of deposit tokens to the auction contract:

- **Investor B bid \$5.2M**
- **Investor C bid \$5M**
- **Investor D bid \$5.3M**

Before bids were placed, the auction contract called for an identity check to perform on-chain verification of each investor. On-chain verification ensured that only verified investors were able to place bids - checking that the investors met transfer agent and fund manager AML/KYC rules and were not on the sanctions list while ensuring that claims were encrypted and private. Investor B and C's identities were successfully verified and their bids were placed, however, Investor D's identity check failed at the sanctions check and therefore, their bid was not submitted.

At auction close, the highest submitted bid won and Investor B was notified. Investor B requested an encrypted \$5.2M of deposit tokens on-chain before the settlement deadline. The auction settled with atomic DvP: Investor B received an encrypted \$5M of Fund A tokens to their stealth address from Investor A (seller). Investor A received \$5.15M of deposit tokens and the fund manager of Fund A received a \$50K (~1%) royalty fee from Investor B for the secondary sale.

**Trust Assumptions:** We maintained key trust assumptions to operate the POC:

- We assumed the role of a trusted operator to deploy essential services.
- We used a trusted key management service (KMS) to securely handle cryptographic keys.
- We relied on a trusted verifier service as an on-chain publisher to request and verify a VP from an investor, checking the DID registry, validating schema and signatures - and ultimately posting results on-chain by extracting encrypted claims.
- We relied on a trusted stealth address service to generate new stealth addresses to maintain anonymity for users as well as to enable selective disclosures through an encrypted allowlist.
- Finally, we also trusted certain actors within the flow - including the bank and transfer agents as issuers of assets within the flow.

**Auditability:** The setup of the POC allows an auditor to view transaction details as required. With the centralized KMS and established trust assumptions, an Operator can decrypt specific transactions for the auditor as needed. Additionally, future enhancements could include granting the auditor with allowlist access to specific smart contracts, which programmatically defines which transactions and contracts an auditor is privy to.

## Advantages

- Confidentiality of transaction balances: fhEVM keeps transaction balances encrypted and unknown to the public.
- Anonymity of addresses: Stealth addresses allowed users involved in a transaction (sender and receiver) to maintain anonymity where new stealth addresses are generated every time a new transaction is conducted - resulting in a user's ability to keep their actions private.

- Reusable and privacy-preserving on-chain investor KYC: By leveraging the Kinexys SSI SDK as well as privacy-preserving technology, a user benefits from an efficient and compliant onboarding experience – and will continue to benefit from those efficiencies throughout the lifecycle of the use case (or additional use cases).

## Scalability considerations

While FHE solutions encrypt transaction balances on-chain, the main bottleneck is scaling to complex business logic due to FHE's computational complexity. This could be potentially addressed with co-processors on each validator that perform FHE computations off-chain and put the results back on-chain to maintain L1 consensus without introducing additional trust assumptions, but more research is to be done here.

Enabling selective disclosures for encrypted transactions is key for institutions to maintain privacy across the ecosystem but allows permitted actors like auditors to be able to access and view certain transactions. In the POC, we implemented a centralized solution with the Stealth Address Service that filters which addresses can call decryption/re-encryption of the transaction balance. For institutional readiness, the ability to enable selective disclosure in a more automated, but flexible way will be key.

Finally, while we were able to make the transaction balance confidential through fhEVM and addresses anonymized through stealth addresses, neither solutions were able to natively shield the token type being transferred between parties, allowing an outside observer to see, for example, that a particular fund was being transacted.

This Privacy Proof of Concept (POC) showcases confidential transactions and computations in asset markets using AvaCloud Privacy Solutions (APS) powered by Avalanche. APS consists of two technologies; Avacy and Distributed Homomorphic Encryption (DHE)<sup>29</sup> for L1s. Avacy provides self-custodial transaction confidentiality and anonymity while ensuring compliance. It leverages zero-knowledge (ZK) proofs to keep account states hidden from third parties. DHE extends Avacy's capabilities to arbitrary secure private computations for smart contracts. Together, combined with Distributed Identity (DID) and Avalanche Warp Messaging, they ensure confidentiality without sacrificing the functionality required for private and secure blockchain-based asset markets. This integrated suite of technologies delivers a highly composable and extensible blockchain solution.

## Implementation overview

### Use Case 1: Streamlining Investor Onboarding

Operators deployed essential contracts for fund tokenization, including fund and cash tokens, auction contracts and governance contracts. Avacy combines zero-knowledge proofs and cryptographic commitments to safeguard balances, transaction details and participant data. Avacy's self-custody design ensures its security relies solely on established cryptographic assumptions.

At deployment, the operator selectively enabled auditors and implemented role-based configurations, granting specific key holders visibility into transaction data. This ensured transfer agents and fund managers maintained appropriate oversight of asset data, while regulators retained full ability to review.

Additionally, investors received on-chain identification through Decentralized Identifier (DID) solutions. These DIDs could then be reused and verified in subsequent transactions, streamlining the onboarding process and reducing the risk of fraud.

### Use Case 2: Capital Deployment into Fund

Investors subscribed into a tokenized fund using Avacy and DID, which protected their subscription amounts and identities of participants. Investor DID proofs were programmatically validated through compliance logic and the smart contract's enforced rule set. This process obscured the requesting investor's address while providing visibility to authorized transfer agents and fund managers, ensuring investor portfolio details remained confidential.

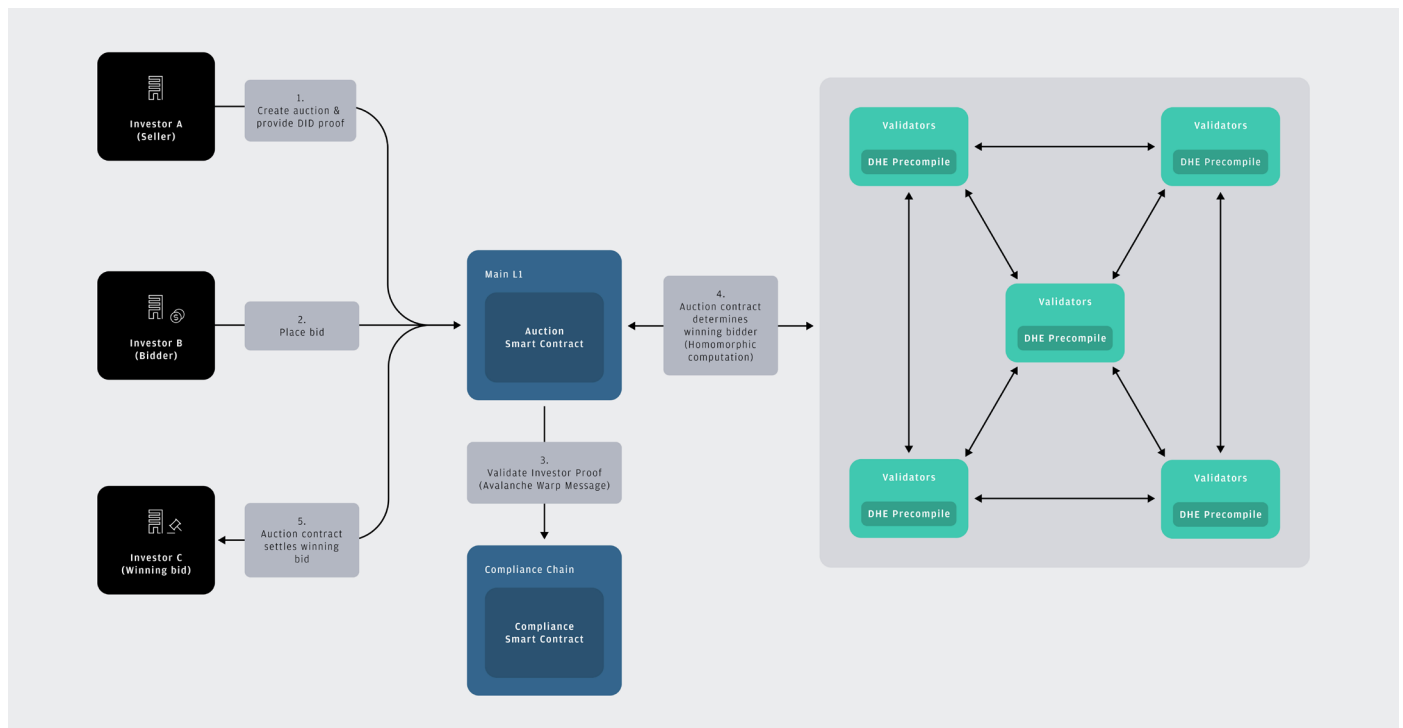
The information in this report, or on which this report is based, has been obtained from sources that the authors and/or J.P. Morgan believe to be reliable and accurate. However, such information has not been independently verified and no representation or warranty, express or implied, is made as to the accuracy or completeness of any information obtained from third parties.

Upon approval, investors could purchase fund assets in a non-custodial manner with obfuscated transaction amounts. To settle this transaction, the issuance of the fund tokens to the investor and the corresponding transfer of cash were executed atomically.

## Use Case 3: Secondary Market Trading

In this use case, market participants securely verified their credentials and account states without disclosing their identities to third parties, submitting the resulting proofs to the auction smart contract. Upon receiving these participation intents, the contract routed encrypted credentials to the compliance chain - a second network specifically for AML/KYC process management, ensuring alignment with on-chain compliance rules. Although not mandatory, the compliance chain enhanced investor onboarding efficiency, overcoming common deterrents found in traditional systems.

In this proof of concept, there was a focus on protecting both investor portfolio composition and market liquidity as investors listed assets for sale and participated in bidding. The auction logic and final settlement were executed using the DHE protocol, enabling full anonymity and confidentiality for all participants. Transfer agents, fund managers, banks, and auditors gained access strictly to the information essential to their roles, preserving privacy across the process. All computations within the Auction smart contract were performed homomorphically, negating the need to decrypt underlying data thanks to the DHE protocol's efficiency. Settlement of the winning bid and fee payments occurred confidentially and atomically within the same block.



The information in this report, or on which this report is based, has been obtained from sources that the authors and/or J.P. Morgan believe to be reliable and accurate. However, such information has not been independently verified and no representation or warranty, express or implied, is made as to the accuracy or completeness of any information obtained from third parties.

## Trust Assumptions

Avacy required minimal trust due to its self-custodial nature, while DHE introduced a trust assumption that nodes would not collude to reconstruct secret keys. However, the system was designed to mitigate this risk through its architecture and by securing critical information with Avacy. DHE is only used to homomorphically process auction-related smart contract operations, while Avacy protects balance and addresses of holders. This means in the event of collusion by DHE nodes, the revealed information would be limited.

## Advantages

- Markets stayed continuously active and accessible, where transactions remained fully protected by DHE and Avacy protocols. Participants did not need to risk exposing their positions or losing a competitive advantage.
- The solution was composable, meaning it could meet the needs of operators who are looking to devise highly specific solutions.
- Auctions utilized a novel DHE system, enabling secure execution of arbitrary computations. By integrating various cryptographic techniques, Avacy achieved higher performance for operations that typically incur significant computational overhead.

## Scalability considerations

- 1 DHE traded off some computation for communication efficiency, causing latency to vary significantly with the geographic distribution of the participating validator set. The current POC offered reasonable performance, but adjustments were needed for institutional need. A globally distributed validator set would impact the potential throughput negatively, in the current phase, institutions would need to co-locate validators in similar regions, but not necessarily in the same data centers.
- 2 Wallet solutions had to ensure investors felt comfortable participating in market activities in a self-custodial manner. For a trustless implementation, users would need to be secure using the technology or abstractions had to be provided without sacrificing security.
- 3 Validator set management for DHE, including key re-sharing, required operational overhead that needed optimization before scaling to a production-ready environment.
- 4 The DHE protocol required validators to have up-to-date knowledge of which other validators were online or offline before beginning any evaluation process. A mechanism was necessary to effectively manage these validator states to ensure system reliability.

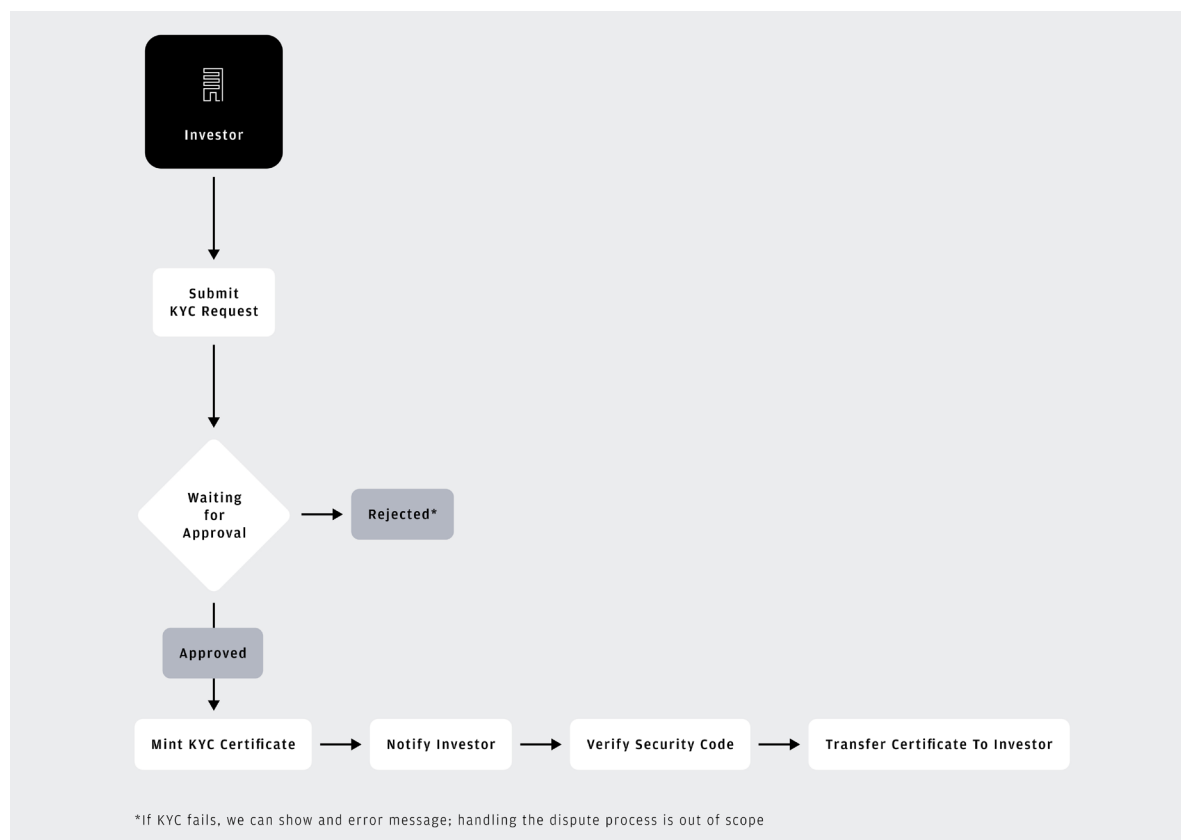
The information in this report, or on which this report is based, has been obtained from sources that the authors and/or J.P. Morgan believe to be reliable and accurate. However, such information has not been independently verified and no representation or warranty, express or implied, is made as to the accuracy or completeness of any information obtained from third parties.



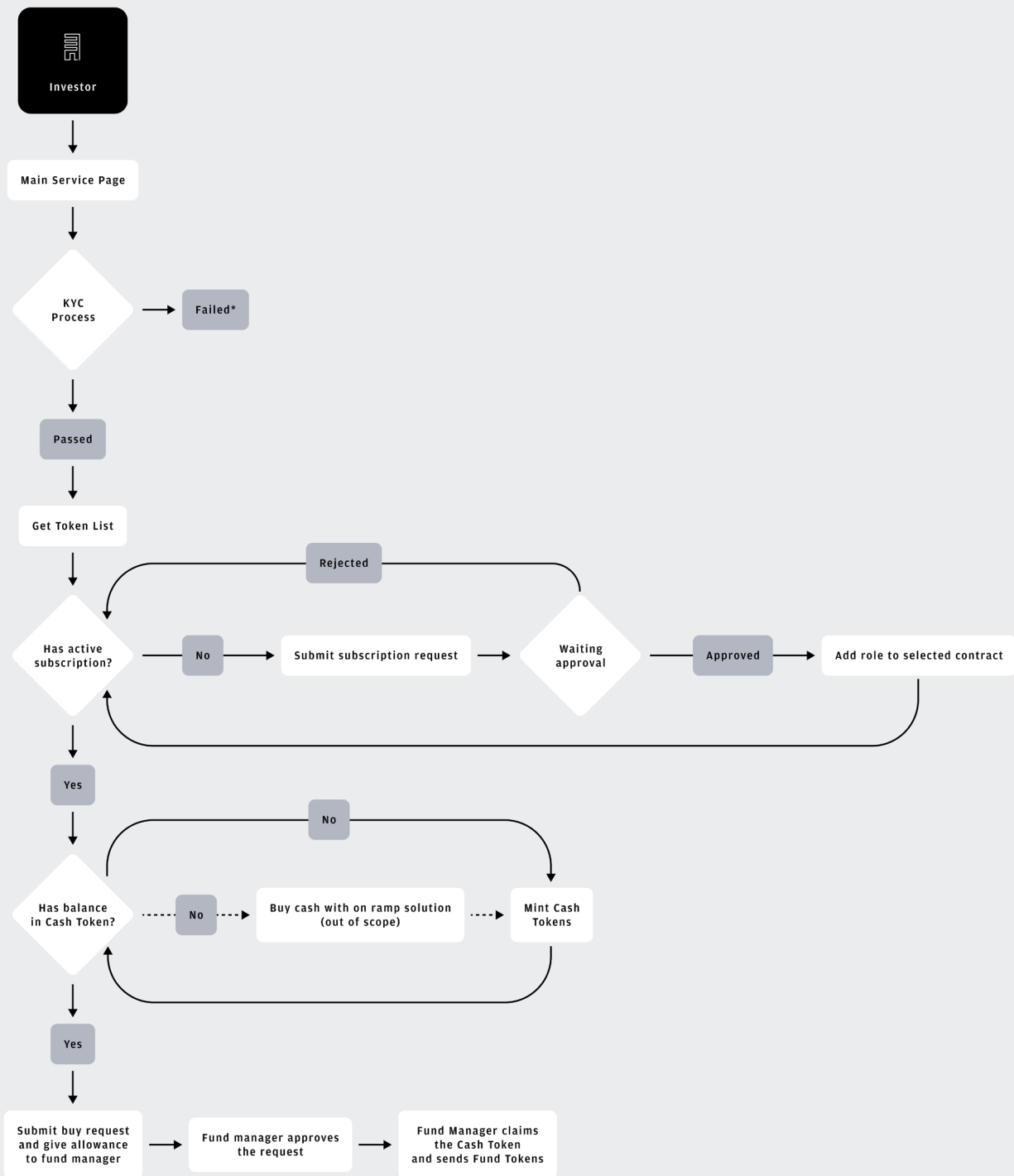
Fhenix is an Ethereum-based leveraged Fully Homomorphic Encryption (FHE) to maintain data confidentiality. FHE allows encrypted data to be processed and computed on without needing to decrypt it, ensuring that sensitive information remained private even during complex operations. This enables secure transactions, including providing funds privately, or more advanced computations in smart contracts without exposing the underlying data.

## Implementation overview

The POC showcased how Fhenix could manage confidential financial data, KYC information and fund management for institutional investors. FHE ensured that sensitive data, such as encrypted balances and KYC certificates, could be processed without decryption. This met the requirements by allowing fund managers to view encrypted balances while maintaining the privacy of investors' data. FHE's ability to perform operations on encrypted data enabled secure management of complex transactions, auctions, and fund subscriptions without exposing underlying information.



The information in this report, or on which this report is based, has been obtained from sources that the authors and/or J.P. Morgan believe to be reliable and accurate. However, such information has not been independently verified and no representation or warranty, express or implied, is made as to the accuracy or completeness of any information obtained from third parties.



\*If KYC fails, we can show an error message; handling the dispute process is out of scope

The information in this report, or on which this report is based, has been obtained from sources that the authors and/or J.P. Morgan believe to be reliable and accurate. However, such information has not been independently verified and no representation or warranty, express or implied, is made as to the accuracy or completeness of any information obtained from third parties.

## Trust Assumptions

- **Operator trust:** The operator was responsible for securely deploying and maintaining the infrastructure. This included setting up KYC and fund management services while correctly applying FHE. The operator needed to have the technical skills to manage encryption securely, preventing data leaks during transactions.
- **Fund issuer/transfer agent trust:** The transfer agent was trusted to manage fund creation (FHERC20 contracts). While processing encrypted data, they had to correctly deploy new funds and follow privacy and security protocols.
- **KYC verification trust:** The KYC process relied on service providers to verify users accurately. Once a KYC certificate was issued, it was assumed to represent the verified identity of the investor. KYC data confidentiality was ensured through encryption, but the accuracy of the KYC process depended on the KYC agent.
- **Smart contract trust:** FHE protected privacy during computations, but there was trust needed in smart contracts to perform as intended. These contracts managed token transfers and interactions, assuming no harmful code existed that could compromise user privacy.

## Advantages

- 1 **Data Security:** FHE kept sensitive institutional data encrypted during computations, which prevented unauthorized access and reduced risk while on-chain.
- 2 **Compliance Readiness:** FHE helped meet data privacy regulations by keeping information private.
- 3 **Versatility:** FHE could be integrated into various institutional workflows, allowing secure computations without compromising data privacy.

## Scalability considerations

The main bottleneck was computational efficiency. FHE required more resources than traditional encryption, which led to slower processing times, especially with large datasets. For institutions that need fast data processing the latency FHE introduces could be a limitation.

Hardware could also pose a challenge. To efficiently process encrypted data, institutions would need to invest in high-performance computing resources, which may not be widely available or economically feasible at scale. Optimizing FHE algorithms for better performance is ongoing and scaling to meet high throughput demands requires future work.

The information in this report, or on which this report is based, has been obtained from sources that the authors and/or J.P. Morgan believe to be reliable and accurate. However, such information has not been independently verified and no representation or warranty, express or implied, is made as to the accuracy or completeness of any information obtained from third parties.

# Global Technology Applied Research, JPMorgan Chase - Private, Auditable and Distributed Ledger (PADL)

PADL is a new, open-sourced<sup>30</sup>, distributed ledger framework with a state-of-the-art design which employs widely used cryptographic primitives combined with zero knowledge proofs to enable fast confidential peer-to-peer multi-asset transactions without any intermediary/trusted party (no-trusted setup). PADL hides the value of tokens with a combined system of a Pedersen commitment and an audit signature. This combined system is publicly verifiable and enables selective disclosures, meaning participants can choose to only reveal transactions to specific parties. PADL comes with a library of cryptographic primitives developed in RUST and an easy-to-use API implemented in Python, that allows a streamlined building of a stand-alone distributed ledger. The PADL smart contract enables an EVM compatible solution with on-chain verification of transactions and composability to enable secondary markets such as private auctions.

## Implementation overview

**Privacy:** PADL's transaction scheme is designed with a 'no-trust setup' meaning PADL doesn't rely on, but can incorporate if required, parties that can decrypt all private transactions. PADL achieves privacy via a combination of public key encryption and zero knowledge proofs. Thus, a participants' transactions and balances are always encrypted. PADL provides multi-asset confidentiality and anonymity meaning participants are not able to learn about other participants asset transactions. Our accompanied whitepaper provides proof for the PADL transaction scheme to be computationally hiding and statistically binding. The PADL token, in principle, is encrypted with Pedersen Commitment and an audit signature, ensuring the correct maintenance of an immutable ledger on-chain.

**Auditability:** PADL supports transaction inspections and selective disclosures via zero knowledge proofs or via opening token values. KYC/AML, trading rules and governance rules are also encrypted and verifiable in a similar manner. Each transaction includes several proofs to assure the transaction integrity; confirmation that assets aren't spent twice, assurance that assets aren't created or lost, verification that transactions remain untampered and auditable and confirmation that the spender has authorized the transaction. Other conditions that can be added are proof of rate/liquidity and traceability. Finally, PADL supports auditing on specific values, that is, the participants can reveal only the requested information without compromising another participant's privacy. This provides full traceability when required.

The information in this report, or on which this report is based, has been obtained from sources that the authors and/or J.P. Morgan believe to be reliable and accurate. However, such information has not been independently verified and no representation or warranty, express or implied, is made as to the accuracy or completeness of any information obtained from third parties.

**Customized privacy (Selective disclosure):** Participants have auditing capability to make their values visible to specific entities in the transaction, by adding ‘audit signatures’ intended for use by the auditing bodies. Using these audit signatures, the auditor can query the value encrypted in the PADL private ledger without having to reveal information about another transaction or asset.

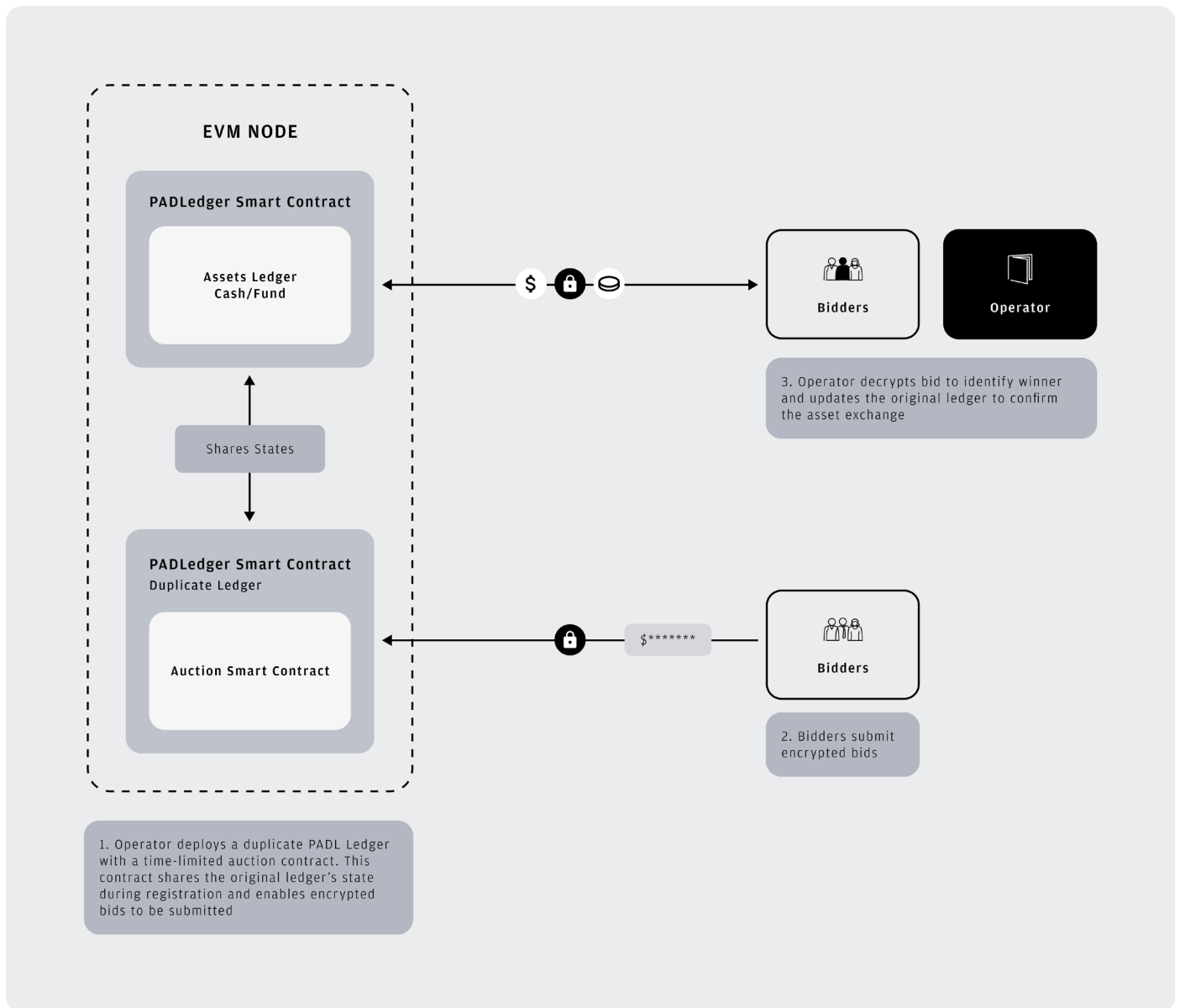
**No-Trusted Setup:** PADL’s transaction scheme does not require a trusted body for set up. It is achieved by using publicly verifiable and extractable tokens. i.e. the party who makes the transaction does not provide the hiding/blending factors, however, other participants are able to recover their own values using their secret/private keys. Specific to the use case:

- Investors do not need to trust other investors: they do not share any information besides their anonymized registration address to the ledger.
- Operator can see bids in auction.
- Transfer agents can verify AML/KYC rules.

Composability and EVM support: PADL smart contract is an EVM compatible smart contract that supports all PADL features, such as the maintenance of balance and state of ledger, allowing participants to check balance and make transfers, the PADL smart contract comes with the ability verify on-chain. This means that PADL smart contract verifies a transaction on-chain before it is accepted. Proof generation is off-chain by design, meaning the participants do not ever have to share their secret key. PADL is able to interact with other smart contracts. This allows for composability, that is, new contracts with new functionality can inherit all the capabilities of PADL smart contract leading to setup of secondary markets such as an auction. In the specified use-case, the PADL smart contract’s multi-asset atomic swap is used for the exchange of cash and fund tokens. The use case also demonstrates an auction smart contract is deployed easily and interacts with the original PADL smart contract. Tokens can also be derived from ERC20 contract and be deployed/traded privately with a PADL smart contract.

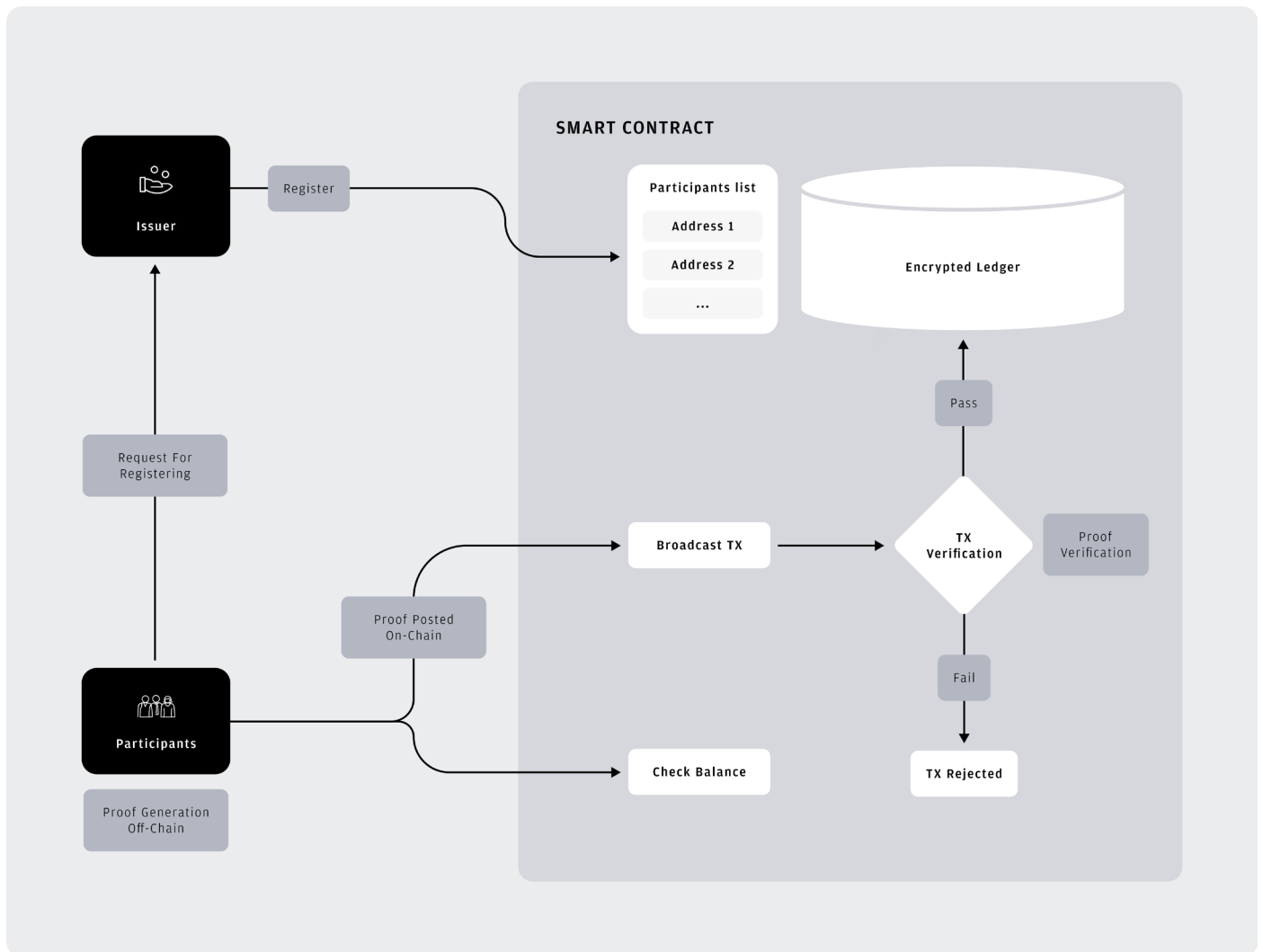
The information in this report, or on which this report is based, has been obtained from sources that the authors and/or J.P. Morgan believe to be reliable and accurate. However, such information has not been independently verified and no representation or warranty, express or implied, is made as to the accuracy or completeness of any information obtained from third parties.

# PADL Smart contract end-client interactions and functionality



The information in this report, or on which this report is based, has been obtained from sources that the authors and/or J.P. Morgan believe to be reliable and accurate. However, such information has not been independently verified and no representation or warranty, express or implied, is made as to the accuracy or completeness of any information obtained from third parties.

# Flow overview of interactions in the use case for two assets



The information in this report, or on which this report is based, has been obtained from sources that the authors and/or J.P. Morgan believe to be reliable and accurate. However, such information has not been independently verified and no representation or warranty, express or implied, is made as to the accuracy or completeness of any information obtained from third parties.

## Advantages

- No trust setup or pre-compiled code, with no validators holding any shared secret key. A flexible solution that is independent of the blockchain infrastructure/consensus that can run on single to many EVM nodes.
- Private multi-asset ledger with selective disclosure auditing that supports on-chain verification, EVM compatibility, atomic swap, composability among many other features.
- Fast transactions compare to other solutions based on other ZKP technology or FHE on native EVM and with no requirement for special hardware.

## Scalability considerations

The main bottleneck in scaling the solution is that the PADL library and API are still in the development phase, and not yet product-ready solutions. It requires further resources to build the library to a deployable product standard with a client facing application. The auction flow required a trusted actor to compare bids and submit transactions but this could be further automated with ZKP range proofs in the future for added privacy.

The information in this report, or on which this report is based, has been obtained from sources that the authors and/or J.P. Morgan believe to be reliable and accurate. However, such information has not been independently verified and no representation or warranty, express or implied, is made as to the accuracy or completeness of any information obtained from third parties.



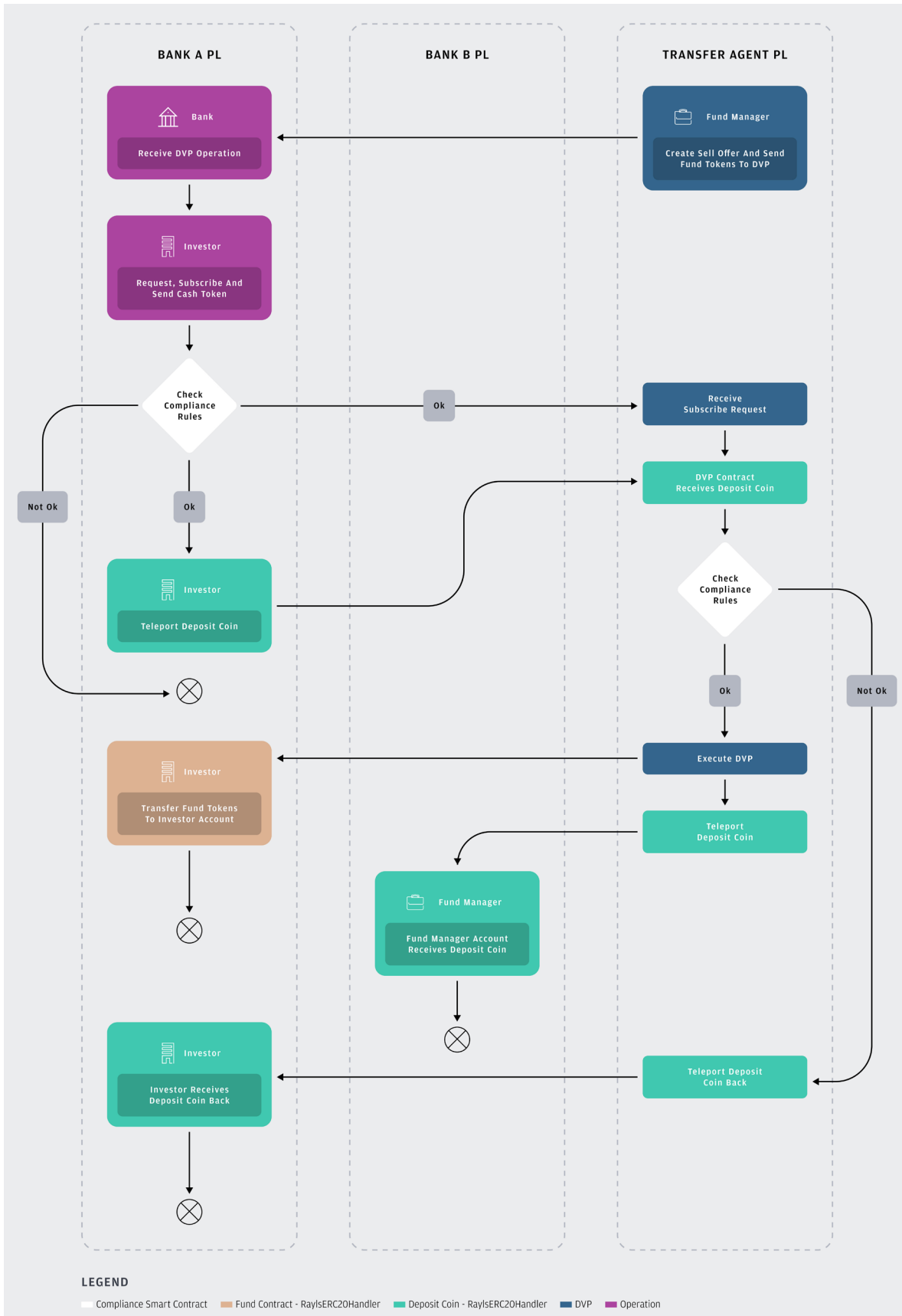
Parfin's privacy solution, Rayls, used permissioned blockchains called 'privacy ledgers' connected through a decentralized blockchain known as the 'commit chain'. The commit chain served as a shared blockchain for privacy ledgers to communicate encrypted messages. Each entity, theoretically, ran its own privacy ledger on-premise and interacted with others through the atomic transport protocol. This protocol involved the sender submitting a Merkle root attestation<sup>31</sup>, indicating accurate ledger updates and an encrypted message tagged for the correct destination ledger. Atomic teleport ensured cross-chain asset transferred correctly, while privacy ledgers maintained independent, confidential records within the network.

## Implementation overview

**Institutional Onboarding:** The onboarding process used Ethereum Attestation Service (EAS) to streamline KYC validation. A bank issued a Merkle root attestation proving an investor's KYC data was part of their larger dataset, shared across subnets as needed. Sensitive data was obscured, with only verifiable proofs exchanged between participants, meeting compliance without unnecessary exposure.

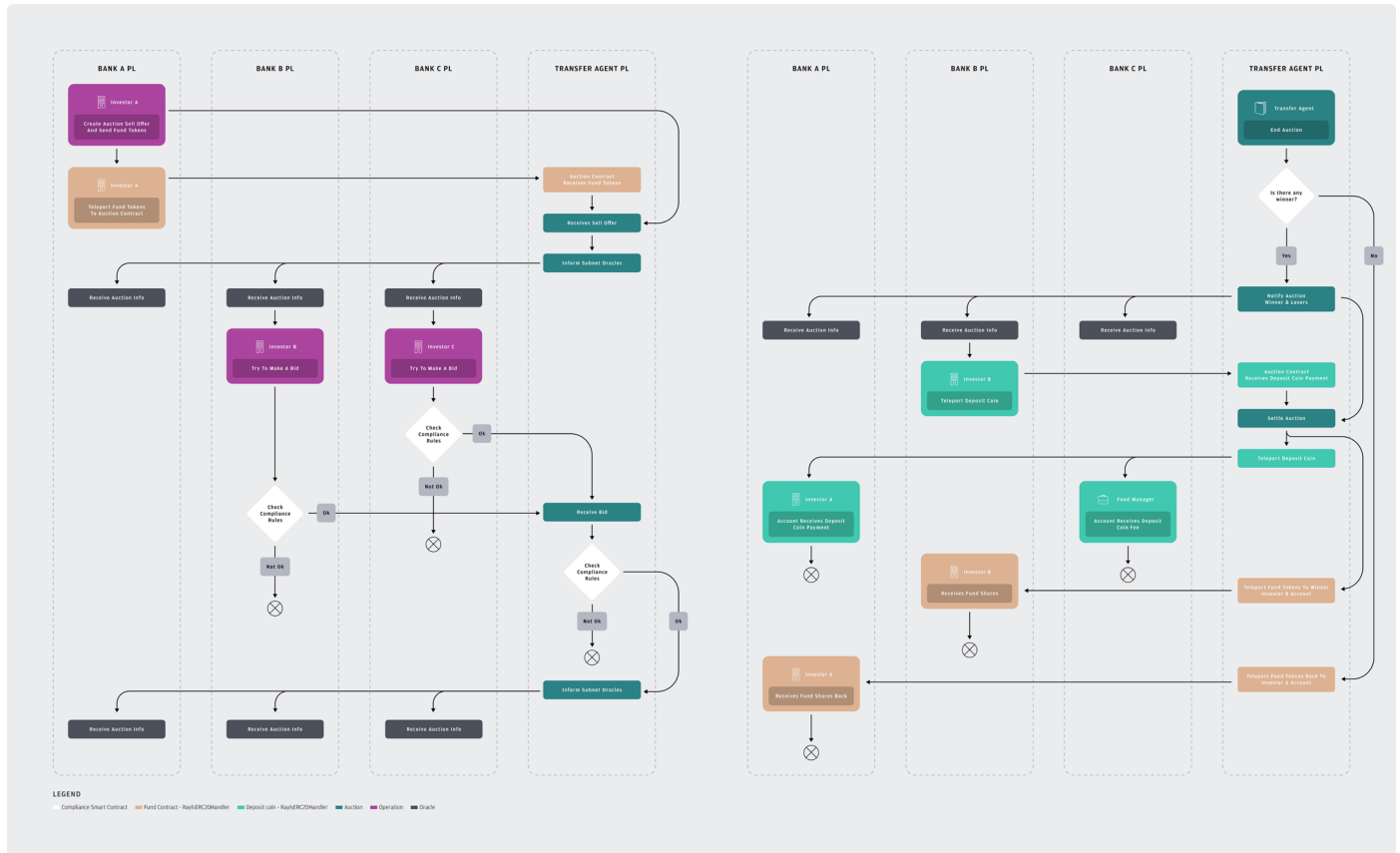
**Fund Subscription Workflow:** Once onboarded, institutional investors exchanged demand deposits for on-chain cash. Subscription requests were processed within private-ledger environments. Atomic Delivery versus Payment (DvP) ensured simultaneous exchange of payment and fund tokens, mitigating counterparty risks. The privacy-ledger design ensured that only authorized entities could view subscription details, while maintaining compliance standards throughout.

The information in this report, or on which this report is based, has been obtained from sources that the authors and/or J.P. Morgan believe to be reliable and accurate. However, such information has not been independently verified and no representation or warranty, express or implied, is made as to the accuracy or completeness of any information obtained from third parties.



The information in this report, or on which this report is based, has been obtained from sources that the authors and/or J.P. Morgan believe to be reliable and accurate. However, such information has not been independently verified and no representation or warranty, express or implied, is made as to the accuracy or completeness of any information obtained from third parties.

**Auction Process and Trust Assumptions:** During auctions, the seller submitted shares to the transfer agent's subnet using atomic teleport. Oracle contracts distributed auction information across subnets, with Merkle root attestations validating bidder eligibility. DvP mechanisms settled the transaction securely between buyer, seller and fund manager. Trust assumed all participants adhered to the subnet compliance rules, with encrypted attestations from the transfer agent deemed sufficient for validation.



## Trust Assumptions

- Private Subnets and Privacy Ledgers:** Rayls uses network topology to segregate data between different institutions who run their own EVM based privacy ledgers. These privacy ledgers can operate independently to manage an institution's own internal tokenized operations and custody their clients' keys.
- Subnet Operator:** The entity that sets up the network, oversees its governance and validates cryptographic proofs.

The information in this report, or on which this report is based, has been obtained from sources that the authors and/or J.P. Morgan believe to be reliable and accurate. However, such information has not been independently verified and no representation or warranty, express or implied, is made as to the accuracy or completeness of any information obtained from third parties.

- **Auditor:** An auditor would use the ‘God View’ functionalities and the ‘Flagger’ component. The God View functionality allows the auditor to access the details of any cross-chain transaction by a specified Privacy Ledger. The Flagger component decrypts the cross-chain transaction data and flags it if a Privacy Ledger attempts to send more than their correct balance.

## Advantages

**Privacy by Design:** Privacy ledgers protected sensitive data on-premise, with end-to-end encryption and Merkle root attestations enabling confidential interactions.

**Regulatory Compliance:** Integrated with AML/KYC frameworks through attestation services, ensuring trust and meeting institutional requirements.

**Interoperability and Scalability:** The modular architecture supported cross-chain transactions via atomic teleport protocol, allowing participation in multiple markets without sacrificing security or privacy.

## Scalability considerations

The primary bottleneck for scaling lies in the cryptographic complexity of the privacy technologies employed. A privacy pool approach using ZKPs instead of Merkle root attestations would provide the added flexibility. The underlying throughput of the commit chain is also a crucial factor for the scaling of our system as a higher number of privacy ledgers in the network requires an acceptable underlying throughput.

The information in this report, or on which this report is based, has been obtained from sources that the authors and/or J.P. Morgan believe to be reliable and accurate. However, such information has not been independently verified and no representation or warranty, express or implied, is made as to the accuracy or completeness of any information obtained from third parties.

# References

- 1 <https://github.com/Consensys/quorum/wiki/ZSL>
- 2 <https://www.jpmorgan.com/insights/payments/wallets/institutional-defi>
- 3 <https://github.com/jpmorganchase/onyx-ssi-sdk>
- 4 <https://www.jpmorgan.com/kinexys/project-guardian>
- 5 The EVM is a decentralized virtual environment that executes code consistently and securely across all nodes. <https://ethereum.org/en/developers/docs/evm/>
- 6 Launch of Blackrock's BUIDL on public Ethereum <https://www.businesswire.com/news/home/20240320771318/en/BlackRock-Launches-Its-First-Tokenized-Fund-BUIDL-on-the-Ethereum-Network>
- 7 [https://app.rwa.xyz/institutional\\_funds](https://app.rwa.xyz/institutional_funds) and <https://app.rwa.xyz/treasuries>, as of October 30, 2024
- 8 <https://defillama.com/> as of October 21, 2024
- 9 <https://www.bcg.com/publications/2023/the-tide-has-changed-for-asset-managers>
- 10 <https://defillama.com/chains/EVM>
- 11 <https://www.jpmorgan.com/onyx/documents/portfolio>
- 12 <https://www.jpmorgan.com/kinexys/content-hub/how-tokenization-can-fuel-opportunity>
- 13 <https://www.bcg.com/publications/2023/the-tide-has-changed-for-asset-managers>
- 14 [https://www.mfs.com/en-us/individual-investor/about-mfs/our-history.html#:~:text=1924,-MFS%20Invents%20First&text=End%20Mutual%20Fund-,On%20March%2021%2C%20MFS%20establishes%20Massachusetts%20Investors%20Trust%20\(MIT\),for%20millions%20of%20everyday%20investors.](https://www.mfs.com/en-us/individual-investor/about-mfs/our-history.html#:~:text=1924,-MFS%20Invents%20First&text=End%20Mutual%20Fund-,On%20March%2021%2C%20MFS%20establishes%20Massachusetts%20Investors%20Trust%20(MIT),for%20millions%20of%20everyday%20investors.)
- 15 <https://app.rwa.xyz/>, as of October 25, 2024
- 16 <https://www.bcg.com/publications/2023/the-tide-has-changed-for-asset-managers>
- 17 <https://blockworks.co/news/tokenization-updates-rwa-summit>
- 18 <https://www.hamiltonlane.com/en-us/news/scope-available-via-secureitize>
- 19 Outsourced Chief Investment Officer platforms are hired to allocate the assets of small and mid-size institutional investors. They generally invest in a combination of funds and securities.
- 20 Form 13F of the Securities and Exchange Commission (SEC) requires investment managers to file their long positions in equities, options, exchange traded funds and certain other securities on a quarterly basis.
- 21 Fenergo: KYC in 2023 Report, <https://www.fenergo.com/kyc-trends>
- 22 The Employee Retirement Income Security Act of 1974 sets a higher standard of care for investment managers in dealing with U.S. Corporate Pension plans.
- 23 Privacy pools refer to on-chain smart contracts which, in contrast to ERC-20's, shield asset ownership.
- 24 <https://eips.ethereum.org/EIPS/eip-5564>

- 25 In blockchain, a block is a collection of transactions that are grouped together, verified and added to the chain in a chronological order.
- 26 The programming language used to write smart contracts on EVM blockchains.
- 27 zkDSL's such as Noir and Circom allow developers to build programs that leverage ZKPs, without knowing advanced cryptography.
- 28 Fully Homomorphic Ethereum Virtual Machine, a distinct approach from 'off-chain' FHE.
- 29 The DHE protocol is a confidential execution solution that leverages a combination of Multiparty Computation (MPC) and (threshold) FHE to facilitate privacy requiring use cases on Avalanche blockchains
- 30 <https://github.com/jpmorganchase/PADL>
- 31 A Merkle root attestation is a cryptographic technique to prove specific data is contained in a larger dataset without revealing the specific data itself.