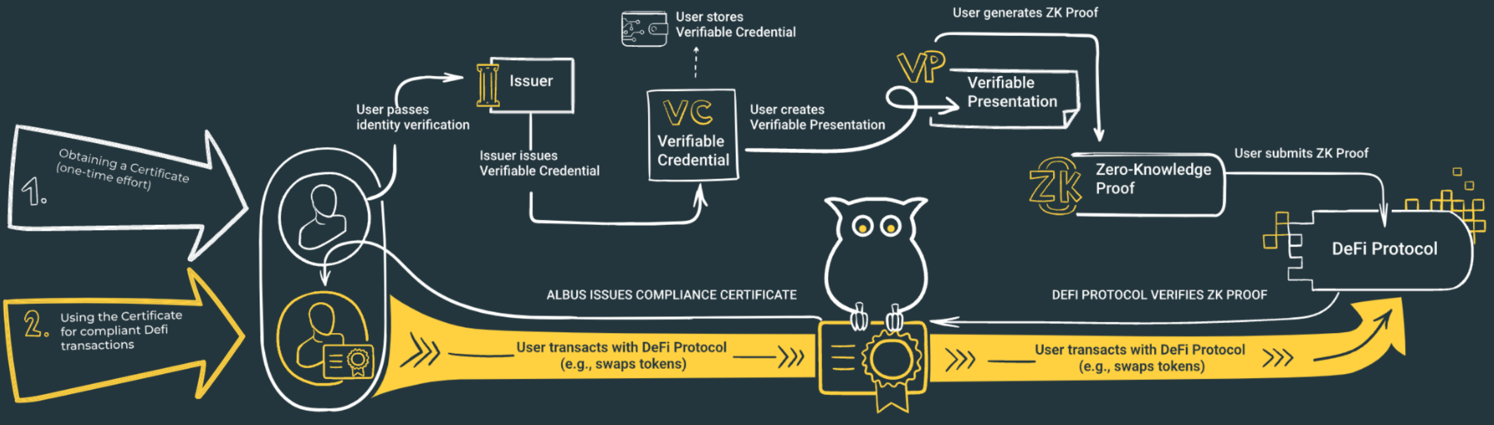
ALBUS PROTOCOL

New opportunities in Web3 through a privacy-oriented approach to KYC/AML compliance

Lite paper V2.02 – September 2023

Albus Protocol is an all-in-one Compliance-as-a-Service solution that facilitates KYC/AML compliance for transactions on public blockchains. Building on a Self-Sovereign Identity (SSI) model, Albus harnesses the power of blockchain and Zero-Knowledge Proof cryptography to enable verification of these transactions in a privacy-oriented manner. This approach brings together the strengths of two worlds: the steps involving human interaction ensure that the verification is conducted as per applicable legal requirements, while the cryptographic mechanisms allow for the results of this verification to be implemented at scale.

HOW IT WORKS


1. Obtaining a Certificate (one-time effort)
2. Using the Certificate for compliant Defi transactions
User passes identity verification
Issuer
Issuer issues Verifiable Credential
User stores Verifiable Credential
VC
Verifiable Credential
User creates Verifiable Presentation
VP
Verifiable Presentation
User generates ZK Proof
ZK
Zero-Knowledge Proof
User submits ZK Proof
DeFi Protocol
ALBUS ISSUES COMPLIANCE CERTIFICATE
DEFI PROTOCOL VERIFIES ZK PROOF
User transacts with DeFi Protocol (e.g., swaps tokens)
User transacts with DeFi Protocol (e.g., swaps tokens)

THE PROBLEM

i. STATUS QUO

For now, Web3 and KYC/AML compliance seem oceans apart. In principle, KYC requirements and the cult of pseudonymity can hardly coexist. Web3 users wish to preserve their privacy, while undergoing KYC verifications is increasingly requested from them.

One aspect of the conflict mentioned above is especially evident in the realm of decentralized finance, or DeFi. DeFi operates on permissionless protocols, which are designed to be public goods. These can be accessed and used by anyone without needing to disclose or verify their identity. Moreover, these protocols are typically governed in a decentralized manner, which means there isn't a central authority overseeing their operation. This leads to public concern about the lack of safeguards against money laundering, financing of terrorism, fraud, and use of proceeds from hacker attacks in DeFi. The promise of decentralized, automated financial services and greater financial inclusion doesn't seem to offset these worries.

Current regulatory developments often aim to extend existing laws and regulations to encompass DeFi. However, a lot of these efforts overlook the unique characteristics of these technologies. In particular, they frequently depend on the concept of a centralized intermediary—a notion that is fundamentally incompatible with DeFi. Consequently, most of these regulations fall short of their intended objectives, leading many DeFi projects to bypass their applicability.

Given this backdrop, a system is needed that ensures KYC/AML compliance for financial transactions on public blockchains, in line with the FATF recommendations, without relying on intermediaries. This is critical to effectively prevent the misuse of blockchains for illegal activities and to significantly enhance trust in the Web3 ecosystem. Such improvements will inevitably encourage the adoption and integration of DeFi protocols. Given the high-speed nature of on-chain transactions, automation is crucial for achieving optimal results, as no human intermediary can keep up.

ii. UNTAPPED POTENTIAL IN DEFI

Many traditional finance (TradFi) market participants, including financial institutions, are increasingly looking to integrate with DeFi protocols, drawn by their potential to address existing inefficiencies and broaden service offering. However, the lack of KYC/AML compliance in the DeFi space is a major hurdle to this integration.

DeFi offers vast potential for institutional players, redefining the traditional financial landscape. According to the 2022 Survey of Global Institutional Clients conducted by Celent, 91% of respondents are willing to invest in tokenized products, and 77% would like to gain access to staking pools to increase their yield on crypto assets. With appropriate compliance practices in place, DeFi platforms could attract considerable investments from the TradFi sector.

Another important opportunity is the trading of security tokens. By expanding into this market, DeFi platforms can unlock new revenue streams and generate additional profits. To be eligible to provide this service on its platform, a DeFi project must meet the regulations that apply to traditional securities, which usually means deploying KYC/AML practices.

Blockchain technology offers quicker, cost-effective solutions for cross-border payments, remittances, and notably, streamlines settlement and clearing processes. By removing traditional intermediaries, such as custodians or clearing houses, DeFi ensures swifter, more efficient transaction processes for TradFi businesses, particularly for international dealings.

To integrate with institutional players, DeFi projects need a solution that ensures rigorous compliance with KYC/AML regulations without compromising user privacy. This solution must include robust user verification mechanisms that align with global KYC/AML standards, mitigating risks of illicit activities. At the same time, it's essential that this solution preserves the privacy of user data and complies with stringent personal data protection regulations. With such a system in place, DeFi projects can demonstrate maturity that institutional investors seek, and become a more appealing and secure investment avenue, potentially unlocking vast new capital inflows into the sector.

OUR SOLUTION

i. ALBUS PROTOCOL

Albus Protocol, or Albus, provides a Compliance-as-a-Service solution for Web3 projects that enables them to be assured of who their users are, without access to their personal data. This opens up vast business opportunities in decentralized finance (DeFi) and other areas of the crypto space, from bringing institutional money on-chain to unlocking the potential of real-world asset tokenisation.

Albus addresses the problem of compliance and user privacy by implementing a unique combination of Self–Sovereign Identity (SSI) principles, Zero-Knowledge Proofs (ZKPs), and secret sharing cryptography.

Albus takes a two-dimensional approach to ensuring that transactions on public blockchains comply with KYC/AML regulations. This approach relies on Self–Sovereign Identity principles to give users control over the data they use to prove who they are, and on Zero-Knowledge Proofs to keep user data private. On the one hand, it allows Web3 users with pre-existing non-custodial wallets to obtain Verifiable Credentials and prove claims contained in them. On the other hand, it allows Web3 projects to verify these claims.Albus employs secret sharing cryptography and introduces the role of a Trustee for ultimate compliance with KYC/AML regulations. In the long term, users will also be able to create new non-custodial wallets through Albus, offering even stronger assurance of KYC/AML compliance.

Albus Protocol can be leveraged by any Web3 project that needs reliable compliance verification, whether it’s a monetary project, such as a DeFi protocol, or a non-monetary one, for example a metaverse. This lite paper focuses on DeFi protocols.

In the case of DeFi, Albus equips the protocols with a capability to verify that their users comply with the policies they set for the specific transactions the users want to conduct. On the user side, Albus allows such a user to prove compliance, while keeping their personal data private throughout the verification process. Users receive a Compliance Certificate that makes them eligible to conduct this specific type of transaction with this specific DeFi protocol. This certificate has a limited validity period set by the DeFi protocol, which forces the user to update the information they provide when the certificate expires. This ultimately results in enhanced efficiency and compliance for DeFi transactions.

Albus Protocol is designed as a blockchain-agnostic solution, meaning it can be deployed on any public blockchain, regardless of whether it's EVM-compatible. Originally, it was deployed on Solana.

The architecture of Albus has been designed to guarantee service continuity, even beyond the lifespan of the initial company that coded and deployed the Protocol.

ii. USER DATA PROVIDERS

Trusted User Data Providers, such as KYC providers, Self-Sovereign Identity (SSI) providers, and other organizations (such as banks and authorities), can issue Verifiable Credentials through Albus Protocol. Notably, Albus collaborates with well-known traditional KYC providers. This collaboration gives each DeFi protocol a wide range of User Data Providers to choose from.

User Data Providers are deemed trusted if the Verifiable Credentials they issue are reliable and can be accepted by DeFi protocols in accordance with the processes required by KYC/AML or other regulations. Furthermore, these User Data Providers must also comply with any industry regulations they are subject to, such as those related to registration requirements, professional diligence, data privacy, and data retention.

To interact with Albus Protocol, each User Data Provider must generate a pair of keys: a public key, which acts as a decentralized identifier, and a private key, which is used to sign the Verifiable Credentials. By signing each Verifiable Credential with its private key, a User Data Provider ensures the Verifiable Credential's traceability. The User Data Provider also formats the credentials based on the W3C Verifiable Credentials Data Model. If the User Data Provider is unable to issue a Verifiable Credential in the correct format, Albus uses a dedicated adapter module that fetches user data from the User Data Provider via API and converts it to a Verifiable Credential. This adapter runs on a so-called Issuer node outside the Albus framework.

iii. VERIFIABLE CREDENTIALS

A Verifiable Credential is a digital document containing a set of verifiable claims that need to be proved. Each user undergoes standard processes with the User Data Provider chosen by a DeFi protocol, for instance traditional KYC verification. The selected provider verifies the information provided by the user, and issues a corresponding Verifiable Credential. The user stores the Verifiable Credential in their wallet (Figure 1).

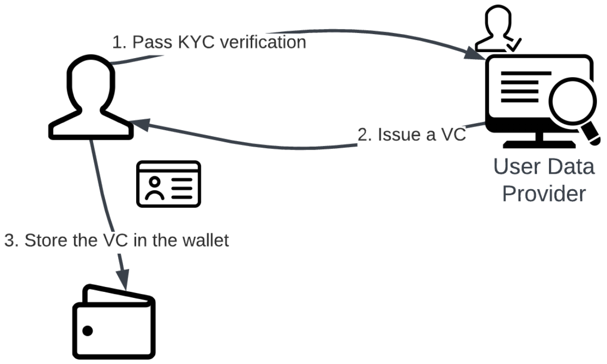


Figure 1. Passing KYC verification and receiving a VC.

Concretely, Verifiable Credentials are stored in an encrypted form on the blockchain. They are added to the metadata of a non-transferable non-fungible token (NFT) that is controlled by the user alone. The user's wallet address serves as a decentralized identifier. As the user obtains additional Verifiable Credentials, they can update the NFT to reflect higher verification levels or to meet the requirements of different jurisdictions.

iv. VERIFIABLE PRESENTATIONS, CIRCUITS, AND ZERO-KNOWLEDGE PROOFS

When a user needs to prove a claim to a DeFi protocol they want to use, they need to create a Verifiable Presentation from their Verifiable Credential. This Verifiable Presentation will contain only the piece of information required for this proof. For example, if a user needs to prove their age, they can use their digital passport stored as a Verifiable Credential to create a Verifiable Presentation containing only their date of birth.

After a Verifiable Presentation is created, an associated cryptographic mechanism called a circuit takes it as input to generate a Zero-Knowledge Proof that allows to prove a claim without disclosing the relevant private data. The generated Zero-Knowledge Proof is stored within the Verifiable Presentation (Figure 2).

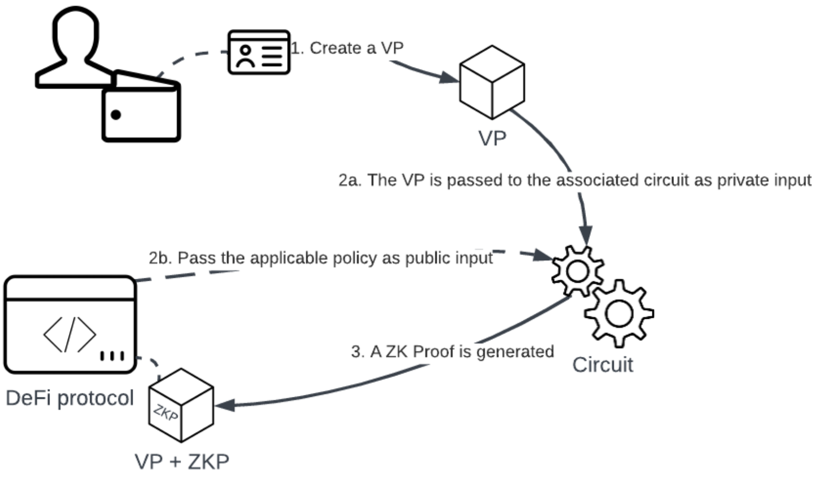

1. Create a VP
VP
2a. The VP is passed to the associated circuit as private input
2b. Pass the applicable policy as public input
3. A ZK Proof is generated
Circuit
DeFi protocol
ZKP
VP + ZKP

Figure 2. Creating a VP and generating a ZK Proof.

A circuit is an arithmetic model designed to generate Zero-Knowledge Proofs. It takes two types of input: private user data from Verifiable Presentations and publicly known data about something that the user needs to prove. For example, if a DeFi protocol requires its users to prove they are over 18 years old, a predefined age circuit is used that takes the user's date of birth from a corresponding Verifiable Presentation as private input and the DeFi protocol's publicly known policy as public input.

The Albus team creates circuits using circom, a circuit programming language, and stores them on-chain. Each circuit represents a specific policy type and is selected by a DeFi protocol when creating a policy in the Albus UI (Figure 3). For example, if a DeFi protocol needs to verify the age of their users, it needs to select a predefined age circuit and specify the age limit.

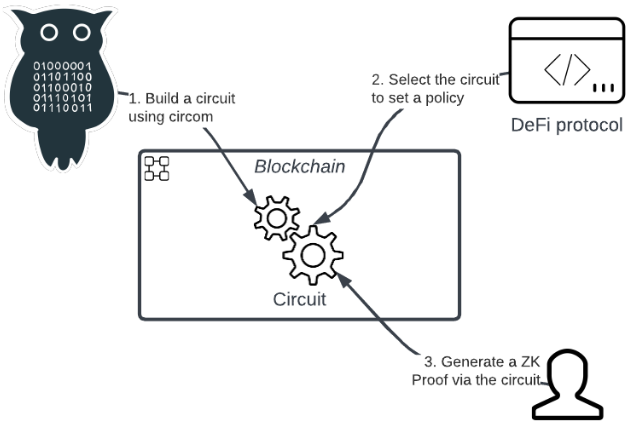

01000001
01101100
01100010
01110101
01110011
1. Build a circuit using circom
2. Select the circuit to set a policy
DeFi protocol
Blockchain
Circuit
3. Generate a ZK Proof via the circuit

Figure 3. Using circuits.

KYC/AML-related compliance requirements transposed through policies often stem from legislation and rules that service providers need to adhere to, or may voluntarily choose to follow, to ensure a safe environment for their users. These requirements might include validating the user's age, citizenship, place of residence, or confirming that the funds involved have not been tainted or blacklisted on-chain.

To ensure that the information provided by users in their Verifiable Credentials remains relevant, Albus allows DeFi protocols to set a validity period for the Compliance Certificates issued to their users, and enables User Data Providers to revoke Verifiable Credentials when an actual document expires or a user's status changes. If a certificate has expired and the original Verifiable Credential used for obtaining this certificate has been revoked, the user has to get another Verifiable Credential by passing identity or other verification with a User Data Provider. This way, the information in the Verifiable Credential is kept up-to-date.

If a particular blockchain does not support Zero-Knowledge Proofs, Albus Protocol can provide an off-chain zero-knowledge proving system and bootstrap the necessary oracle for this purpose.

v. WORKFLOW

After a DeFi protocol is onboarded to Albus, it creates a policy by selecting a corresponding circuit. At this step, the protocol sets a validity period for the Compliance Certificates issued to users upon successful verification of their compliance with the policy, and a retention period for the Verifiable Presentations created by these users.

When a user initiates a transaction with the DeFi protocol, Albus is requested to verify if this user complies with the policy. Albus checks if a Compliance Certificate containing the required Zero-Knowledge Proof already exists. If not, it checks if the user has the Verifiable Credential to create a Verifiable Presentation, generate the required Zero-Knowledge Proof, and receive the certificate. If not, it initiates a procedure for obtaining a Verifiable Credential through a User Data Provider. Only after Albus Protocol confirms that the user complies with the policy can the DeFi protocol execute the transaction.

Example: Consider a gambling protocol that needs to verify if its users are at least 18 years old. The protocol can set the appropriate age policy based on a predefined age circuit provided by Albus, or it can contact Albus to request a custom-made circuit. After this, a user who wants to use the protocol's gambling service can create a Verifiable Presentation and generate a Zero-Knowledge Proof of compliance with the age policy. When it happens, the user receives a Compliance Certificate that allows them to use this specific service of the gambling protocol.

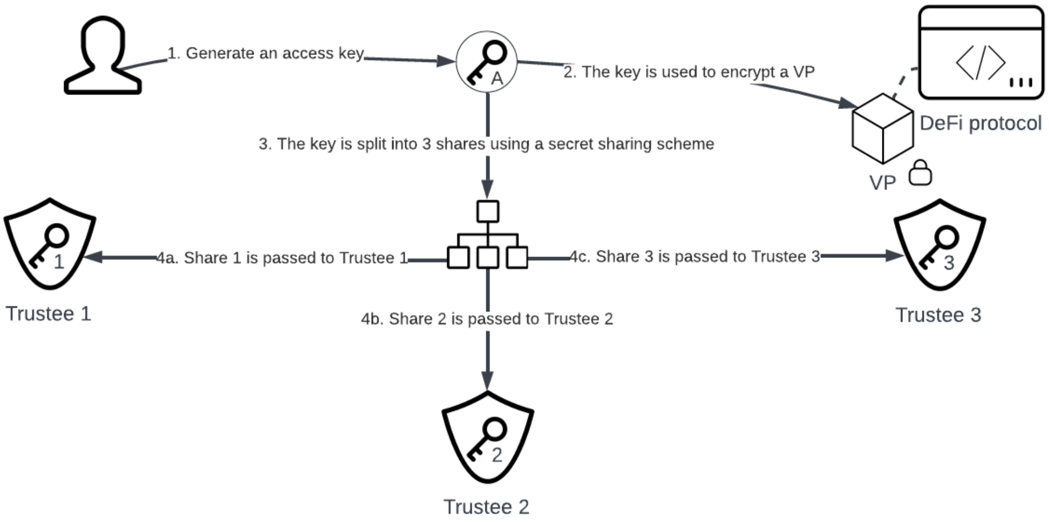
If a particular blockchain does not support Zero-Knowledge Proofs, Albus Protocol can provide an off-chain zero-knowledge proving system and bootstrap the necessary oracle for this purpose.

If there are no circuits available for a specific policy, the Albus team can create a custom-made circuit upon request tailored to this policy.

vi. SECRET SHARING AND TRUSTEES

Albus Protocol applies a secret sharing scheme and introduces the role of a Trustee to ensure that user data subject to KYC/AML regulations can be accessed by a government authority upon legitimate request, for example as part of an ongoing investigation or an audit.

Each Verifiable Presentation containing personal data of a user is encrypted and stored on-chain. Albus utilizes a secret sharing scheme that involves splitting the key required to decrypt the Verifiable Presentation into multiple shares and passing each share to a Trustee (Figure 4). After the split, the key can be reconstructed using a specific number of these shares, for example two out of three. This scheme ensures that the user's personal data cannot be accessed arbitrarily by a single party but can be made accessible to government authorities as they need it.



1. Generate an access key
A
2. The key is used to encrypt a VP
DeFi protocol
VP
3. The key is split into 3 shares using a secret sharing scheme
4a. Share 1 is passed to Trustee 1
4c. Share 3 is passed to Trustee 3
4b. Share 2 is passed to Trustee 2
1
Trustee 1
3
Trustee 3
2
Trustee 2

Figure 4. Splitting an access key and distributing its shares between Trustees.

A Trustee is a trusted third-party entity that acts as a safekeeper of one of the key shares and is established in each jurisdiction covered by Albus Protocol to handle all compliance-related inquiries from the authorities of this jurisdiction. A Trustee can be represented by an organization that specializes in compliance or regulatory affairs.

If a fiscal or any other government authority presents a legitimate request for access to a user's personal data in a Verifiable Presentation, a set number of key shares held by Trustees are combined to generate the key for decrypting the data and fulfilling the request (Figure 5).

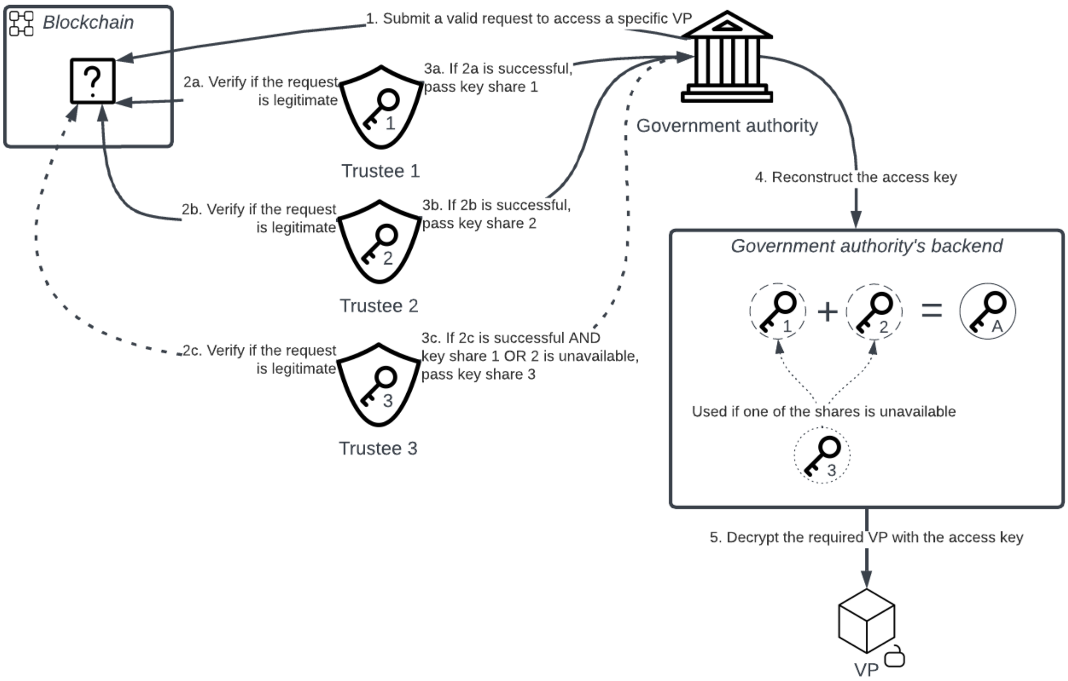

Blockchain
?
1. Submit a valid request to access a specific VP
2a. Verify if the request is legitimate
3a. If 2a is successful, pass key share 1
1
Trustee 1
Government authority
2b. Verify if the request is legitimate
3b. If 2b is successful, pass key share 2
2
Trustee 2
4. Reconstruct the access key
Government authority's backend
1
+
2
=
A
Used if one of the shares is unavailable
3
2c. Verify if the request is legitimate
3c. If 2c is successful AND key share 1 OR 2 is unavailable, pass key share 3
3
Trustee 3
5. Decrypt the required VP with the access key
VP

Figure 5. Reconstructing the access key and decrypting user data.

Users can always decrypt and access the data in their Verifiable Presentations, for example, to verify its accuracy. However, for compliance reasons, Verifiable Presentations are controlled not by users but by the DeFi protocols they interact with. The DeFi protocols have to store the Verifiable Presentations for a certain period of time defined by applicable regulations. This period is called a retention period and can be set by a DeFi protocol for each policy it configures through Albus. The Verifiable Presentations generated by a user can be automatically deleted when the applicable retention period expires. If a Verifiable Presentation is stored on-chain, the access to it can be disabled by requesting each party of the secret sharing scheme to delete its key share.

The system outlined above allows for a broader ecosystem that blocks funds based on red flags raised by User Data Providers. If a User Data Provider rejects the issuance of a Verifiable Credential, it may lead to a refusal of funds from all DeFi protocols that rely on certificates issued by Albus for the Verifiable Credentials from that User Data Provider. In contrast, in traditional systems, users would resubmit information to each service provider, who then processes it through their own User Data Provider. If one service provider raises a red flag, the user may adjust their documentation or seek more lenient service providers. In this context, a single red flag does not necessarily lead to multiple gates closing, whereas one refused certificate can result in many gates closing.

KEY FEATURES IN BRIEF

i. Users maintain access to their private data in Verifiable Credentials and presentations at all times.
ii. Neither Albus Protocol nor any DeFi protocol with which a user interacts has access to the user's private data.
iii. Private data can be retrieved upon a valid request from any authorised entity, including financial intermediaries, which ensures that the system aligns with KYC/AML requirements.
iv. DeFi protocols have the autonomy to select User Data Providers they trust and want to work with, rather than being compelled to accept proofs generated from untrusted data.
v. In the future, the product will continue to function independently of the company.
vi. For enhanced compliance, a fully compliant ecosystem can be established, in which all assets are traceable from the moment they are introduced into the ecosystem.

Note: There are a number of features planned for implementation in the future. You can find their description in the Appendix to this lite paper.

ADVANTAGES

i. New opportunities: We pave the way for our clients to draw liquidity from institutionals and TradFi and to tap into the burgeoning market of security tokens, including tokenised real-world assets (RWA). We provide the infrastructure for comprehensive compliance on public blockchains, enabling businesses to explore new avenues for growth.
ii. Guaranteed privacy for users: Trust is paramount. With our implementation of Zero-Knowledge Proofs, we ensure that user data remains private, making it inaccessible not only to the DeFi protocol a user interacts with but also to Albus.
iii. User targeting without compromising privacy: With Albus, Web3 businesses can gain insights into user behaviours and attributes using Zero-Knowledge Proofs. This allows for tailored targeting strategies and personalized user experiences, all while ensuring absolute data privacy. Instead of accessing raw data, businesses can determine specific user characteristics, for example a particular demographic group, ensuring that engagement is both effective and respectful of user confidentiality.
iv. Future-proof business: As stringent KYC/AML regulations take shape in numerous jurisdictions, Albus positions businesses at the forefront of compliance, ready to navigate the new regulatory landscape.
v. Compliance-as-a-Service solution with shared benefits: Through the Albus Compliance-as-a-Service offering, we eliminate the need for businesses to incur the costs of developing and implementing in-house compliance solutions. The broader Albus ecosystem provides two distinctive benefits.

Firstly, It lets DeFi protocols access a shared pool of users with reusable Compliance Certificates, which reduces the cost of verification. Secondly, through its infrastructure layer, it enables liquidity sharing across DeFi protocols seeking compliance.

vi. Safer smart contracts: We prioritize the security of your smart contracts. Every user is verified before they can engage with your protocol. This identity verification significantly reduces the threat of exploitation or hacker intrusions. By adding this layer of protection, we ensure that malicious actors are less likely to act without facing consequences, which boosts the overall resilience of your smart contracts.

vii. All-in-one solution: Albus provides a comprehensive platform, catering to all KYC/AML compliance needs. While we prioritize user data privacy, we also ensure it's readily available for legal scrutiny upon valid request.

APPENDIX: POTENTIAL FEATURES

This Appendix describes potential features considered for implementation in the future.

i. USER’S TRUST SCORE

Zero-knowledge proofs can be utilized to establish a risk-based model, providing a trust score for each user in the context of their interactions with a given DeFi protocol. The scoring model can be tailored to the needs of each DeFi protocol or asset provider. The system's design ensures that the exact formulas implemented within the risk model are not disclosed to the public.

Concretely, the above allows for transactions to be blocked if a user's trust score falls below the threshold specified for that particular transaction, even if there are no specific factors directly prohibiting its execution.

In such instances, a manual review of the transaction is initiated. The transaction is then escalated to an appropriate authority, who may ultimately approve or reject the transaction.

ii. RANDOM KYC CHECKS

Albus can introduce random KYC checks to improve the security of the DeFi ecosystem. Periodically and unpredictably, Albus may prompt users to pass KYC verification, which could range from taking a selfie to other advanced verification mechanisms. By doing so, Albus can ensure continuous trust and deter malicious activities.

These random KYC checks ensure that a DeFi platform’s trust in a user is periodically reaffirmed, keeping user profiles authentic and offering a continuous trust mechanism beyond initial registration. Such checks also introduce uncertainty and unpredictability, deterring malicious actors from identity theft, account takeovers, and other forms of digital fraud.

iii. VERIFIED NON-CUSTODIAL WALLETS

Instead of simply obtaining a Verifiable Credential from an available User Data Provider, Albus will at a later stage allow for verified wallets to be created via the Albus infrastructure. Given that Albus is blockchain-agnostic, such wallets will be compatible with any blockchain. The verified wallets inherently enable compliance, as they come with embedded functions that permit transactions only with other compliant wallets, or verified protocols that passed a KYB check. As a result, ”ring-fenced compliant ecosystems” will be made possible, where every asset in circulation is fully compliant.