zkKYC in DeFi

An approach for implementing the zkKYC solution concept in Decentralized Finance

Pieter Pauwels
Independent Researcher
pieterpauwels@protonmail.com

Joni Pirovich
BADASL
info@badasl.com

Peter Braunz
Independent Researcher
pbraunz@gmail.com

Jack Deeb
Mycelium
jack@mycelium.ventures

March, 2022
Version 1.0

Abstract

Decentralized Finance (DeFi) protocols have triggered a paradigm shift in the world of finance: intermediaries as known in traditional finance risk becoming redundant because DeFi creates an inherent state of "trustlessness"; financial transactions are executed in a deterministic, trustless and censorship resistant manner; the individual is granted verifiability, control and sovereignty. This creates challenges for compliance with jurisdictional Anti-Money Laundering and Combatting the Financing of Terrorism (AML/CFT) regulations, including Know-Your-Customer (KYC) policies, given that no personal information should be shared and stored on public, transparent blockchains. This paper presents a solution concept for where a DeFi protocol is required or finds it desirable to implement KYC policies. zkKYC in DeFi requires no personal identifiable information to be shared with DeFi protocols for the purpose of regulatory transparency. The presented approach extends the zkKYC solution concept (which leverages self-sovereign identity and zero-knowledge proofs) with the introduction of KYC Issuers and Decentralized Oracle Networks (DONs) as key solution components. KYC Issuers verify the identity of an individual, but have no knowledge about their digital asset wallets or DeFi activity. DeFi protocols interact with digital asset wallets, but have no knowledge about the identity of the individual controlling them. If and when deemed necessary, only a designated governance entity is able to reveal the identity of an individual that is under strong suspicion of being a bad actor in a DeFi protocol. The presented solution architecture demonstrates flexibility in being agnostic to blockchain platforms and SSI implementations and extensibility in being forward compatible with on-chain identity and reputation systems. Similar to the original zkKYC solution concept, zkKYC in DeFi breaks the regulatory transparency vs. user privacy trade-off.

Keywords: zkKYC; decentralized finance (DeFi); privacy; AML/CFT; know-your-customer (KYC); zero-knowledge proof (ZKP); self-sovereign identity (SSI)

1 Introduction

Background This paper follows the zkKYC paper published mid 2021 [1]. The majority of interest in and feedback about that paper focused on how the presented solution concept could be applied to Decentralized Finance (DeFi). This broad interest warrants exploration of the motivations for applying zkKYC to DeFi protocols as well as how it could be best applied across different DeFi use cases and implementations. The authors acknowledge that many DeFi protocols and projects operate to preserve and enhance user privacy. This paper does not attempt to wrest that viewpoint. It rather attempts to explore the zkKYC solution concept as a KYC policy for DeFi projects that wish to preserve and enhance user privacy and simultaneously reduce counterparty risk or ensure criminal or other suspicious behaviour is deterred from their DeFi protocol.

Context Digital technologies are increasingly disrupting different areas of our modern society. Two decades ago, the Internet started to disrupt the media and communications industries. Next, the introduction of online payments created a boom in e-commerce and has fundamentally changed the face of business and (retail) commerce. Over the last few years, the number of projects adopting blockchain technology has set a pace for disruption of the financial services industry and even money itself. A proliferation of digital assets and DeFi are the result. The full potential and the consequences of this technology for the financial services industry and other industry verticals are yet to be determined.

DeFi has experienced explosive growth since early 2020. The Total Value Locked (TVL) in DeFi protocols on the Ethereum blockchain reached 1 billion USD for the first time in June 2020. In September 2021 TVL on Ethereum reached over 140 billion USD [2]. In the same time period, the number of unique addresses interacting with DeFi protocols increased from 200,000 to over 3,000,000 [3]. The initial growth originated from experiments within the crypto community itself, but it quickly triggered broader interest, not least due to the opportunity for high returns compared to traditional finance. In 2021 institutional investors started to pay attention as well. Most recently, progressive FinTech companies are exploring the integration of DeFi services into their traditional offerings (CeFi-DeFi bridges) with the view of launching in early to mid 2022. Even large banks are expanding their offerings, with the Commonwealth Bank of Australia - that has over 50% market share of Australian customers - recently announcing that it will allow its customers to buy, hold and sell digital assets through its CommBank app. [4]

The DeFi industry has a false reputation for being mostly unregulated to date because of the lack of up-to-date guidance from regulators and lack of enforcement action. Such lack of guidance and enforcement activity has created a belief, and in some cases a legitimate expectation, that the law is unclear and DeFi protocols are truly operating in “the grey”. Without consumer and investor complaints, it is difficult for a regulator to justify the allocation of finite resources to enforcement activity. However, regulators and law makers around the world are starting to lean into DeFi with objectives to protect investors, prevent the activities of bad actors and minimize the creation of risk (including systemic risk as the values locked and transacted in DeFi grow exponentially relative to the existing 350 trillion USD global financial system). Some of this increased interest by regulators is no doubt also driven by the rise in DeFi exploits, hacks and fraud. According to blockchain analytics firm Elliptic, losses due to theft and crime across DeFi protocols in 2021 have increased by over 600% from 2020, with more than 10 billion USD being stolen in 2021 compared with 1.5 billion USD in 2020 [5].

As with the early days of the Internet, the decentralized and permissionless nature of the technology makes it very challenging to apply traditional concepts and analogies to this nascent industry. Regulation to detect and prevent financial crime and that promotes financial market infrastructure safety and soundness principles has traditionally relied on centralized intermediaries which may have been, but no longer are, technology neutral. This regulation must be revised to be applicable to the new global, decentralized and permissionless business models possible because of blockchain technology.

Objectives This paper aims to present an approach to apply the zkKYC solution concept to DeFi protocols without compromising the zkKYC premise of simultaneously providing the requested (regulatory) transparency as well as fully protecting user privacy. That is, no personal identifiable information must be shared with DeFi protocols for the purpose of transparency and yet, if and when deemed necessary, a designated governance authority must be able to reveal the identity of a DeFi user that is under strong suspicion of being a bad actor.

It is not the authors’ objective to advocate for the introduction of “as-is” KYC policies in DeFi protocols. Rather, where a DeFi protocol is required by regulation or finds it desirable to implement financial crime policies for the “cleanliness” and attractiveness of its ecosystem, this paper suggests an approach that maximises user privacy and aligns with the ecosystem expectation of openness, composability and trust minimisation.

Additionally, it is the authors’ objective to:

- present a suggested approach that leverages existing real-world identities and KYC verification, rather than expecting users to go through this process again for a particular DeFi protocol.
- explore how zkKYC can support anticipated on-chain identities and reputation (crypto or digitally native) and extend and co-exist with off-chain identities and an individual’s data. In so doing, this paper considers the sovereign human individual as the centre and off-chain or on-chain identities as merely credentials issued to them and managed by them.
- educate the industry, regulators and policy makers about the difficulties for DeFi protocols to comply with existing Anti-Money Laundering and Combatting the Financing of Terrorism (AML/CFT) rules and proposed recommendations by the Financial Action Task Force (FATF) relating to virtual assets and virtual asset services providers. The authors express serious concern about the justification and effectiveness of imposing “as-is” KYC requirements onto DeFi protocols. Such a measure, in the authors’ view, would lead to broad non-compliance and/or introduce “trusted” intermediaries that break the DeFi spirit and broader crypto ethos to build a more transparent, reliable and trustworthy global business and financial market infrastructure.

2 Problem Statement

The current financial crime regulation is designed to be applied to centralized intermediaries of financial markets. Such intermediaries are harder to identify in DeFi, or not even present at all. This disintermediation is a key efficiency characteristic of DeFi that allows for faster, less expensive and more accessible financial services to more people. The infrastructure on which these DeFi protocols operate provides a level of transparency that is unseen in traditional finance, yet the identity of the participants is pseudonymous (or anonymous even). It can feel like the opposite of traditional finance, where identities of participants are known, but the system itself is very opaque, closed and lacks transparency. Therefore, the problem is achieving the objectives of the current financial crime regulation (i.e. KYC policies in context of AML/CFT) while respecting the characteristics, nature and spirit of DeFi protocols as well as the public, transparent infrastructure they operate on. This challenge requires addressing the perceived trade-offs between decentralized finance, KYC policies and privacy. Each of these elements is explored more in detail below.

2.1 Decentralized Finance (DeFi)

The ubiquity of and reliance on technology within financial services organisations has been increasing steadily over the last few decades. With the advent of blockchain technology and especially smart contract capabilities, this trend of disruption of the traditional financial industry has further accelerated. Where FinTech [6] mainly disrupted the customer experience of financial services and introduced new players that manage this customer interaction, blockchain technology and DeFi have the potential to disrupt the financial industry at its core by disintermediating financial markets and creating an entirely new financial market infrastructure.

DeFi protocols have been launched and are being built to perform the key functions of a financial system. They are available on public, permissionless blockchain systems and do not rely on trusted intermediaries (e.g. banks, brokers, clearing houses) to facilitate financial transactions and reduce financial risk between counterparties but rather on software applications deployed on a blockchain (i.e. smart contracts). These smart contracts operate autonomously as programmed and their performance is verified by the decentralized network of nodes supporting the blockchain. Smart contracts encode the terms, conditions and logic of the financial product or service, or plainly the rules that participants of a financial transaction agree to. The autonomous nature of smart contracts renders intermediaries as we know them redundant because an inherent state of "trustlessness" is created. The only thing standing between multiple counterparties of financial transactions is public software executed in a deterministic, trustless and censorship-resistant manner. The individual is granted verifiability, control and sovereignty.

DeFi protocols provide transparency on the public blockchain of the financial service logic, the transactions, the market structure and the leveraged exposure (if any). Advanced analytics capabilities are being built to interpret the publicly available information and apply it to an evolving understanding of the volatility of money, financial stability and the safety and soundness of the new global financial market infrastructure. Whilst this public transparency provides verifiability of the system and a new and powerful dataset for regulators to identify financial crime risks and bad behaviour, it also creates challenges to preserve the privacy and safety of participants.

Below is a list of DeFi protocol categories [7] that is considered in scope for the purpose of this paper:

- **Stablecoins** (e.g. USDC, DAI): digital assets that are pegged to the value of a real-world asset, e.g. USD.
- **Decentralized Exchanges (DEX)** (e.g. Uniswap, Curve): exchange digital assets in a decentralized and permissionless manner without giving up custody of your assets.
- **Lending and Borrowing** (e.g. Aave, Compound): lend and borrow digital assets in return for an interest rate that is calculated on market conditions.
- **Insurance** (e.g. Nexus Mutual, Opyn): pay a premium to receive guaranteed compensation under certain conditions of events occurring such as smart contract failures or loss of deposits.
- **Yield Aggregation** (e.g. Yearn.Finance, Harvest): earn optimised yield by depositing digital assets into yield aggregators who constantly move the digital assets to the DeFi protocol that earns the most yield.
- **Derivatives** (e.g. Synthetix, Tracer): create on-chain exposure to digital or real-world assets.
- **Margin Trading** (e.g. dYdX): use borrowed funds (i.e. leverage) to increase a position (and thereby exposure) to a particular asset.

The power (as well as one of the biggest risks) of DeFi is derived from its composability. DeFi protocols represent financial primitives, which are core building blocks of financial markets. They can easily be integrated and composed into powerful new and higher order financial propositions that are not possible in traditional finance. An example of this is flash loans [8]. Flash loans enable you to borrow instantly without the need for collateral, provided that the borrowed funds are returned to the pool within one blockchain transaction. If this does not happen, the whole transaction is reversed to effectively undo the actions executed until that point. Either everything succeeds or nothing. The borrowed (and returned) funds can, for example, be used to benefit from unique arbitrage opportunities across DeFi protocols. In general terms, any financial service implemented in smart contracts can be considered in scope of DeFi for the purpose of this paper.

2.2 Know-Your-Customer (KYC)

Policies In general, businesses can implement a range of KYC policies for different legislated or voluntary commercial reasons (or a combination of both):

- **Customer eligibility**: A business implements a policy that specifies the customer eligibility criteria. This policy might originate from the business itself, but often it is mandated by legislation. A typical example is that specific products (e.g. alcohol, tobacco) can only be sold to customers above a certain age. In this scenario the extent to which a business needs to 'know' their customers is very limited, i.e. whether or not their customers are older than the specified age threshold. KYC is here more about verifying certain claims about the customer, and not about personal identifiable information as such.
- **Operational risk management**: A business that engages in high value or high-risk transactions with their customers, has good reason to manage its counterparty risk and therefore require customer identification. If an adversarial situation arises, legal action can be pursued against the identified customer.
- **Regulatory compliance**: To comply with AML/CFT regulation, a business might be obliged to implement formal KYC policies (e.g. in Australia, as part of an AML/CTF Program [9]). Depending on the jurisdiction a business is located in, this typically involves defining a customer acceptance policy, implementing customer identification procedures, monitoring (and reporting suspicious) customer transactions and setting up a risk management policy.

This paper focuses on KYC policies for the purpose of regulatory compliance such as AML/CFT regulation. The reason for this focus is that such KYC policies will have to meet the strictest (regulatory) requirements. An approach to apply zkKYC for such policies will also be applicable to any other KYC policy. Feedback from the DeFi community has indicated an expectation that (regulatory) KYC obligations might be required under certain circumstances and teams want to explore privacy enhancing options in preparation for impending legislation.

AML/CFT Regulation Broadly, AML/CFT regulation mandates the implementation of financial crime management including KYC policies for providers of "designated services", or more plainly "persons" that provide financial services, bullion services, gambling services or other prescribed services in financial markets. The regulation seeks to mandatorily enlist "persons" to collect personal information to aid regulators in the identification of actors involved in financial crime and bringing enforcement action against those actors. The existence of such a regime is also intended to act as a deterrent for financial crime.

The form of AML/CFT legislation implemented differs between jurisdictions but is generally based on the recommendations and principles set down by the Financial Action Task Force (FATF). For the most part, a KYC policy, as part of an AML/CFT Program, is standardised but for the financial crime risks that are specific to a particular "person" and their services, and the specific mitigation activities undertaken with respect to each risk. To comply with AML/CFT regulatory obligations, customers of these "persons" are required to share their personal identifiable information (i.e. name, date of birth, residential address) so that their identity can be verified, their risk assessed (e.g. by verifying against (international) sanctions or watch lists (e.g. US Office of Foreign Assets Control (OFAC) Specially Designated Nationals list)) and access to the service can be granted accordingly. This personal information collection and risk analysis process is referred to as Customer Due Diligence (CDD) and in certain cases an entity will have to undertake Enhanced Customer Due Diligence (ECDD). "Knowing" your customer, and the risk profile of your customer, is not an initial and static process, it is an ongoing one; hence, the need for Ongoing Customer Due Diligence (OCDD).

Application to DeFi Most, if not all, DeFi protocols are in substance providing financial services that AML/CFT regulation seeks to regulate or has oversight of. However, these protocols usually lack a clear "issuer" or "operator" that maintain authority, control or influence over the protocol and its community and that is or each are a legal person under the relevant law. Under existing AML/CFT regulation, it is unclear who the "person" is to which the law should apply and whether all individuals involved in the development, governance, maintenance, or passive token holding, or a smaller contingent, are carrying on a financial services business in a jurisdiction and are also resident of that jurisdiction. Where a number of individuals around the world make up the "person" as might be the case if all governance token holders in a DeFi protocol comprise a partnership or an unincorporated association (which each qualify as "persons"), it can be difficult for a regulator to determine which individuals are carrying on a financial services business let alone whether a business is being carried on when the provision of the financial product or service is automated. It is challenging to define how traditional regulations exactly fit into and are relevant in detecting and preventing financial crime in this new world of open and decentralized finance. The legal characterisation of an autonomous DeFi protocol – whether or not the protocol is subject to a model of oversight and governance or reflects a previous version of the protocol still living on-chain without oversight or governance – and whether the protocol can qualify as a "person" under AML/CFT regulation is the critical task at hand for regulators and policymakers. Whether or not that task is accomplished, this paper provides zkKYC as a privacy enhancing approach to deterring and identifying bad actors and enforcing financial crime policies in DeFi protocols. Regulators' resources have to date been prioritised to deal with issues and financial crime in traditional finance rather than DeFi. In addition, blockchain analytics service providers have been working with governments, agencies and regulators to effectively identify, track and seize digital assets being used in criminal or other suspicious activity [10], which has largely relied on a point at which a "person"'s on-chain activity can be linked to their real-world identity and location.

This paper focuses on retail individuals as DeFi users, not businesses. The main motivation for focusing on retail individuals is that businesses are more likely to rely on custodians and trusted intermediaries to interact with DeFi protocols. As such these intermediaries are known entities, much smaller in number as DeFi users and their business customers will likely have passed KYC verification already because the custodian or intermediary is providing a regulated financial service that already requires a KYC policy. In the context of digital assets and DeFi, regulators have also expressed a strong interest in protecting retail investors.

Potential harm, ineffectiveness and unintended consequences The use of "as-is" KYC to link personal information with publicly available on-chain activity, relationships and digital asset wealth is not upholding or enhancing an individual's privacy and could pose greater risk to individuals and their physical and digital safety than the current KYC requirements do in traditional finance. Similarly, amending current AML/CFT regulation to apply "as-is" KYC to DeFi protocols by introducing a broad definition of virtual asset services provider (VASP) could result in the AML/CFT regulation making too great a trade-off against harms being made possible against individuals due to their personal information being readily available and not being able to appropriately fulfil its objectives in the DeFi industry to provide for measures to detect, deter and disrupt money laundering, the financing of terrorism and other serious financial crimes.

DeFi protocols are not opaque as their counterparts in centralized financial institutions and the openness and transparency of blockchain transactions is a new development that financial crime policy makers must adapt to. Recent examples have demonstrated that a DeFi protocol knowing the identity of the participants is not necessary to detect financial crime and bring sufficient pressure to bear on bad actors to return the proceeds of crime (i.e. stolen digital assets) and so disrupt the course of financial crime [11]. Finally, every DeFi protocol is configurable, so it can be set whether re-checks are conducted every month or more frequently and can be extended to include list checking or checking of other identity and risk profile metrics. This re-validates the 'identity' and potentially also 'risk profile factors' for the person that has been KYC'd. The authors acknowledge that the trustless, decentralized and transparent nature of blockchain technology on which DeFi protocols run, creates new challenges for identification and management of financial crime that this paper aims to address.

Reputation and decentralized regulation It can be anticipated that along with the design of financial markets also the design of regulation will evolve over time and decentralize in order to improve effectiveness and efficiency. Leveraging the transparency of public blockchains, on-chain reputation systems could be developed that inform (financial crime) risk scoring systems. One can see similarities in Uber or Airbnb where the scoring of participants informs decision making and discourages undesirable behaviour [12]. KYC policies in DeFi could foresee the possibility for "regulation by (on-chain) reputation" and support such evolution, enabling the combination of both real-world identity and on-chain reputation, if found desirable (e.g. privacy impact).

2.3 Privacy

With the proliferation of digital technologies in every aspect of our life, privacy is an increasingly important and hotly debated topic. While privacy itself exists on a continuum, the positions taken in discussions can be very binary. The 'nothing to hide' argument [13] is a good example of this. Privacy is a matter of trade-offs and, in the context of AML/CFT, an individual's right to privacy is traded off against the safety and integrity of the financial system as a whole. In these situations, there is a risk of a reflexive response from policy makers to prioritise the interest of the collective above the rights of the individual, based on a legacy understanding of a financial system that is comprised of centralized intermediaries which does not hold with open, permissionless, blockchain-based technology. This creates opportunities for innovation to step in and break such trade-offs.

Addressing privacy in the context of DeFi, and public permissionless blockchains in general, does create additional challenges given the transparent nature of most blockchains. Transaction details are visible and the usage pattern of a particular wallet address reveals a lot of information about the finances and transaction history of the wallet owner, especially if that wallet is being used across multiple DeFi protocols. Given this transparency, it is a critical challenge to carefully design privacy enhancing KYC solutions. An intuitive approach is to centrally link a wallet address to an individual's verified identity. This approach seems effective but also creates new risks towards privacy if not designed correctly. Collection, storage and sharing of personal information by DeFi protocols could create more harm and unintended consequences, due to the transparency and the increasing prevalence of spear phishing attacks against individuals known to have significant digital assets in their wallet(s). It is also worth noting that blockchain transparency is the means to allow network participants to agree on the validity and the single source of truth. The ability to verify the validity of transactions in a permissionless manner is what creates the trustless nature of blockchains. Technologies such as zero-knowledge proofs can provide this verifiability without transparency about the underlying transaction, and so enhance privacy.

3 Solution Concept

3.1 zkKYC

Before presenting the suggested approach to apply zkKYC to DeFi, it is valuable to revisit the zkKYC solution concept. A detailed description can be found in the zkKYC paper [1]. This section provides a summary overview.

Overview zkKYC extends the self-sovereign identity model, leveraging verifiable credentials (VC) and decentralized identifiers (DID). The key improvement is that individuals (i.e. Holders) no longer have to provide personal identifiable information to each business (i.e. Verifier) that they create a relationship with. This is achieved using a circular ecosystem design with clear role definitions and modern technologies, including zero-knowledge proofs.

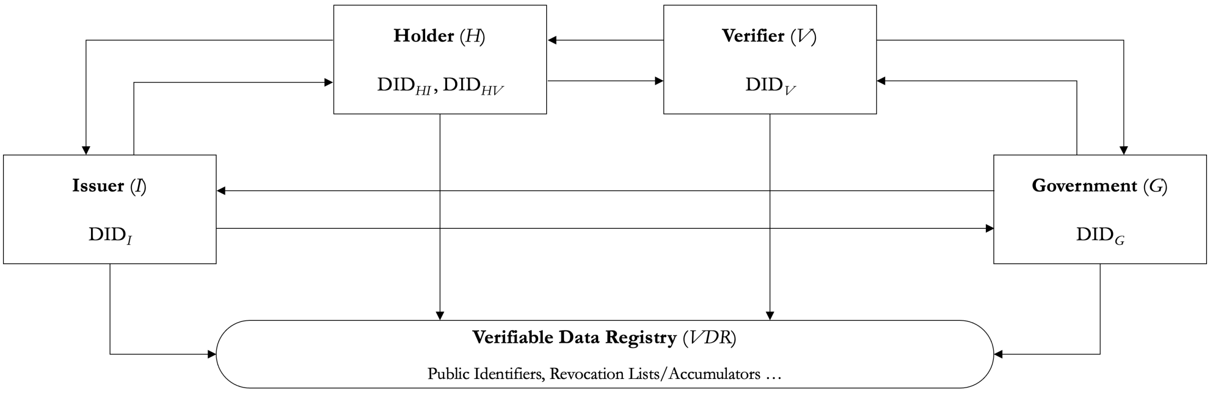

Figure 1: zkKYC overview

Interactions and Concepts Trustworthy Issuers issue verifiable credentials to Holders. Verifiable credentials provide a mechanism to express traditional credentials digitally, cryptographically secure, privacy respecting and machine-verifiable. The Issuer cryptographically signs verifiable credentials with the secret key associated with their decentralized identifier (DID$_I$). Using the publicly available public key associated with the Issuer's DID, anyone can easily verify the integrity and authenticity of a verifiable credential that Issuer issued. Where a Holder is an individual, they would typically generate a unique DID for each distinct relationship they have. This helps to enhance their privacy, as only they then know and control the link between all these different DIDs. In the diagram above, you can see that Holder has DID$_{HI}$ for its relationship with Issuer and DID$_{HV}$ for its relationship with Verifier. In zkKYC, Holders do not present to Verifiers the actual verifiable credentials that were issued to them. This could share personal identifiable information. Rather, Holders use the verifiable credentials in their digital identity wallet to generate and present the following three objects to Verifier:

- **Eligibility Proofs**: zero-knowledge proof that the Holder meets the (business) criteria set out by the Verifier to be able to provide access to the requested service. These proofs leverage the information in verifiable credentials and their signatures, but without disclosing the actual information itself. Examples include proof that the Holder is above a minimum age, a domestic resident, not on a sanctions list, not a politically exposed person etc.
- **zkKYC token**: an encrypted data object that contains decentralized identifiers (DIDs) to enable the Holder's identity to be revealed to parties in Government role only. Specifically, it is a data object encrypted with Government's public key. The data object contains DID$_I$, DID$_{HI}$, DID$_V$ and DID$_{HV}$. DID$_V$ and DID$_{HV}$ make the token unique and specific to Verifier so they are of no value to others.
- **Validity Proofs**: zero-knowledge proof that the presented zkKYC token contains the correct information, without disclosing what that information is, and is encrypted using the provided Government public key. Given that Verifier cannot read the content of the zkKYC token, they need proof that the correct information is included, to prevent bad actors from inserting false information.

As a result, Verifiers do not have any personal identifiable information about their users/customers. They do have decentralized identifiers (DID$_{HV}$), cryptographic proof (eligibility and validity proof) and an encrypted data object (zkKYC token). If and when the need arises (e.g. legal charges, regulatory reporting), a Verifier can present DID$_{HV}$ along with the zkKYC token to Government. Only Government will be able to read the token to identify the originating Issuer(s) of the credential(s) used to generate the token from (i.e. DID$_I$). Read access to the token will also reveal the Holder identifier towards that Issuer (i.e. DID$_{HI}$), which enables the originating Issuer to provide Government with the personal information about the Holder associated with that Holder identifier to pursue their investigation or legal action. The reason why resolving the Holder's identity is assigned to the Government role and not a Verifier is to make sure this is a trusted authority with an assigned governance and oversight responsibility (in pursuit of structured transparency) and to preserve the privacy characteristic that Issuers do not learn the Verifiers at which Holders present their issued credentials. The circular model together with the definition of the different roles defines the ecosystem design. It is designed so that, in pursuit of transparency, the identity of bad actors can be revealed if and when necessary, but that for privacy reasons large scale surveillance of users is not possible. Government can only reveal a bad actor's identity, if both the relevant Verifier and Issuer cooperate.

Outcomes zkKYC builds on top of self-sovereign identity and eliminates the need for personal identifiable information to be shared with Verifiers for the purpose of KYC. Verifiers can verify that their customers meet specific criteria to avoid bad actors from accessing their services. Additionally, the identity of bad actors can be revealed at a future point in time, if their behaviour or transaction pattern has been found to be criminal or fraudulent. The identity and privacy of good actors, that adhere to the jurisdictional laws and regulations, is fully protected and their security and safety enhanced due to less or no personal identifiable information being shared or misused.

3.2 Requirements

The table below lists the requirements that any approach to implement zkKYC in DeFi should meet. Naturally, they extend the requirements that the zkKYC concept as such already realises.

ID	Requirement
REQ-01	**Extend upon zkKYC business requirements.** The requirements for applying zkKYC to DeFi must extend the underlying zkKYC business requirements (see section 3.3 of the zkKYC paper [1]). Applied to DeFi protocols, these are: • The level of user control, agency and privacy provided and enabled by the self-sovereign identity model must be preserved or enhanced. • A DeFi user should not share personal identifiable information (e.g. name, address, date of birth) when on-boarding at a DeFi protocol. • A DeFi user must prove they meet the criteria defined by the DeFi protocol or relevant regulator(s) to consume the provided service (e.g. adult, domestic resident ...). • A DeFi protocol that suspects a specific user of fraud, money laundering or terrorism financing must be able to report that user to Government (e.g. regulator). • A DeFi protocol that wants to file charges against a specific user due to breach of contract or other dispute must be able to report that user to Government (e.g. law enforcement). • Government (e.g. regulator, law enforcement) must be able to identify a reported DeFi user based on the information provided and on the ground of strong suspicion. • When a DeFi protocol reports a DeFi user to Government, this must not be disclosed to the user (i.e. tipping-off). • A DeFi protocol should not hold personal identifiable information on their users, unless it is provided to them by Government in context of a reported issue.
REQ-02	**User centricity and control** While this requirement is reflected in REQ-01, it is worthwhile repeating that any solution concept must put the DeFi user at the centre and in full control. The Holder must be in control of their Verifiable Credentials, stored in a self-sovereign identity (SSI) wallet. In addition, the user must control any digital assets that they want to transact with in a DeFi protocol. This translates into a non-custodial digital asset wallet. As the user is in full control, they may choose to set up and manage multiple wallets for their verifiable credentials and digital assets. Last, only the Holder should be aware of the linkage between their personal identifiable information (stored in verifiable credentials in their SSI wallet) and the digital asset wallets they use to transact with on-chain. This key requirement puts the user in control and protects their privacy.
REQ-03	**Trust minimisation** Applying the zkKYC solution concept to DeFi must align with the DeFi ethos of minimising trust assumptions. There should be no reliance on a centralized solution component, unless under direct and full control of the DeFi user. This also means that any zkKYC ecosystem for DeFi should include an extensive and diverse set of parties that takes up the role of Issuer. A limited or homogeneous set of Issuers risks creating a gatekeeper to the ecosystem as users require a credential from at least one of them.

ID	Requirement
REQ-04	**Interface agnostic** The solution concept must not include any particular assumptions regarding the interface for the Holder to interact with zkKYC or the DeFi protocol. The interactions may take place via a web site, an app, or directly via APIs.
REQ-05	**Blockchain agnostic** It is expected that multiple blockchain platforms will continue to host DeFi protocols. Therefore, any approach to implement zkKYC in DeFi must be blockchain (technology) agnostic.
REQ-06	**Self-sovereign identity platform agnostic** Self-sovereign identity is based on open standards (i.e. verifiable credentials, decentralized identifiers) and multiple implementations have been created. The suggested solution concept should not assume any particular implementation or DID method (and associated Verifiable Data Registry (VDR)). It must be possible for an individual to hold and use verifiable credentials that are associated with decentralized identifiers anchored via different DID methods, in different VDRs.
REQ-07	**Leverage existing KYC processes and outcomes** One of the most frustrating experiences is having to prove your identity over and over again, at every (regulated) service you want to interact with. The ability to re-use the outcome of KYC verification at multiple businesses (i.e. DeFi protocols) is a powerful proposition, for users (convenience) and DeFi protocols (cost). Given their transparent and permissionless nature, DeFi protocols themselves cannot verify the identity and store personal identifiable information of its users. Therefore, assuming the regulatory permission to do so, zkKYC for DeFi should leverage existing KYC processes and outcomes. This requirement will result in broader re-usability of KYC credentials, not just for DeFi protocols, but for centralized businesses alike.
REQ-08	**Ongoing Customer Due Diligence** In addition to Customer Due Diligence at the time of customer onboarding, zkKYC for DeFi must also support Ongoing Customer Due Diligence. The risk profile of a DeFi user might evolve during their lifecycle and it must be possible for DeFi protocols to respond to that appropriately. It is also a fundamental part of financial crime regulation to establish strong ongoing customer due diligence processes.
REQ-09	**Extensibility for on-chain identity and reputation** One can anticipate a future where someone's identity is not purely defined by real-world constructs but also by digital and on-chain native metrics. In a world where communities, pseudonyms and decentralized governance extend nation states, legal identity and corporate governance, a different approach might be preferred (although unlikely for the purpose of AML/CFT in the short term). Therefore, zkKYC for DeFi should be extensible to include these future forms of identity such as reputation scores or other identity related attributes assigned by protocols, DAOs or community members.
REQ-10	**Minimal impact on DeFi smart contracts** zkKYC for DeFi must reduce the impact on DeFi protocol smart contracts to an absolute minimum. Existing smart contracts have often been extensively audited and reviewed for bugs and security vulnerabilities. Including a zkKYC verification step should be limited to one function call with a pass/no-pass response and should avoid impacting to existing smart contract APIs.
REQ-11	**Built-in commercial model** An ecosystem with multiple actors and technology providers requires a fair and balanced incentive model to be sustainable over time. zkKYC for DeFi must provide a built-in commercial model that can automate transfers of value between actors based on their participation and the use case at hand.
REQ-12	**Support for privacy-first (DeFi) protocols** Privacy-first protocols, including those that provide full anonymity, might be considered unlikely candidates for AML/CFT compliance, perhaps even a contradictio in terminis. Yet, to not support malicious activity or not welcome bad actors, they might choose to implement zkKYC to make sure their users pass the strictest regulatory requirements. The degree to which transaction privacy is protected depends on the design of the particular DeFi protocol, but zkKYC should support these protocols if they desire to do so. Note that these protocols might have to accommodate more changes to their smart contracts to integrate zkKYC, for example in case the sender of the transaction is kept anonymous on-chain.

Table 1: Requirements

3.3 Design Considerations

Informed by the requirements outlined above, this section presents a few design considerations that are instrumental for the suggested approach to implement zkKYC in DeFi.

KYC Issuer The zkKYC model includes the role of Issuer. This role is typically fulfilled by widely recognised and trusted entities in the ecosystem. An Issuer is considered authorised to issue Holders verifiable credentials that describe identity related claims about them. zkKYC applied to DeFi assumes a particular type of Issuer and credential that they issue; a KYC Issuer that issues KYC credentials (see also section 5.1 of the zkKYC paper [1]). A KYC Issuer is an Issuer that is qualified to perform KYC activities and has implemented KYC processes that meet jurisdictional AML/CFT requirements. This makes centralized cryptocurrency exchanges, traditional financial organisations or other trusted organisations that implement high quality KYC processes strong candidates to take up this role. Upon successful KYC verification of an individual, a KYC Issuer issues them a KYC credential that describes the KYC outcome. While the details of this credential are to be specified in a future detailed design of any implementation and such details are to be standardised as part of ecosystem governance, they likely (at least) include the following verified information elements:

Information element	Description
Issuer DID (DID_I)	The public DID of the Issuer, published in the Verifiable Data Registry, along with the associated DID Document.
Subject DID (DID_{HI})	The private DID of the Holder towards a particular Issuer. This DID is only known to the Holder and Issuer.
Name	The full name of the Holder.
Date of birth	The date of birth of the Holder.
Address	The residential address of the Holder.
Identification assurance level	The level of assurance of the identification process applied by the Issuer. The different levels must be specified and standardised via zkKYC ecosystem governance.
Date and time of issuance	The date and time of issuance of the KYC credential.
PEP	Is the Holder a politically exposed person?
Sanctions lists	Against which sanctions lists has the Holder been verified?

Table 2: KYC credential

Customer Due Diligence processes are required to be performed at the time of customer onboarding. Because they assess a customer risk profile at a particular moment in time, regulators also mandate ongoing CDD, throughout the customer lifecycle. KYC Issuers are therefore required to regularly review the claims about Holders and revoke an issued credential if no longer correct or valid. Verifiers are able to verify the revocation status of credentials using the Verifiable Data Registry.

The main benefit of the KYC Issuer role is that resources are applied more efficiently by re-using the outcome of highly specialised processes that require a particular expertise and set of technologies. If KYC Issuers are rewarded for their effort, they might specialise even more and create economies of scale. This also creates a risk. If the role of KYC Issuer becomes too specialised and hard to fulfill, the set of parties that are willing or able to pursue this role might become too limited. This risks creating “gatekeepers” to the ecosystem. In addition to a large number, also a diverse set of KYC Issuers is required, to achieve accessibility and inclusiveness. Everyone in society must be able to participate.

Note that KYC Issuers are solely focused on the identity of their customers and unaware of the digital asset wallets they might use. This segregation helps to protect user privacy and is a major differentiator with many KYC solutions that exist today in DeFi that know both the real-world identity and the digital asset wallets used by their customers.

Protocols and Interfaces When we talk about DeFi, we talk about DeFi protocols, consisting of one or more smart contracts on a public, permissionless blockchain. Usually, the developers of a DeFi protocol also create a web-based interface for users to interact with their protocol. Some (also) create a mobile application. But the permissionless nature of DeFi protocols enables their services to be consumed in many different ways and the user can choose how they prefer to do so. Users can write their own smart contract to interact with the Defi protocol smart contract(s). They could also create and deploy their own web interface. Other DeFi protocols could leverage the composability and integrate the DeFi protocol into their own. This permissionless, decentralized nature of DeFi protocols make it more challenging to manage and control user access. A decision by Uniswap Labs (the team that developed the Uniswap DeFi protocol) in July 2021 illustrates this point perfectly [14]. Citing an evolving regulatory landscape, they had restricted access to particular liquidity pools of the protocol via the web interface[1] that they had developed. For many users this web site was their default interface to the Uniswap protocol. This decision made it very clear that the interface was centralized and in full control of the Uniswap Labs team. However, it had no bearing on the fully decentralized Uniswap protocol itself, or on any other interface to the protocol. For many this was a valuable learning experience about the distinction between protocol and interface.

The table below provides an overview of the different types of interfaces a user could have at their disposal to interact with a DeFi protocol. They represent options and it depends on the particular DeFi protocol which of these options are available and how many instances for each exist.

Interface type	Description	Custodian	DeFi Protocol's user
Intermediary	The intermediary provides the interface to the underlying DeFi protocol. The user might not even know or realise they are interacting with a DeFi protocol. E.g.: TradFi, CeFi (BlockFi, Celsius . . .)	Intermediary	Intermediary The Intermediary is the party interacting with the DeFi protocol.
Graphical	The user uses a graphical interface (web site, app) to interact with the DeFi protocol. This can be a DeFi protocol specific interface or from an aggregator (interacting with multiple protocols). E.g.: Uniswap website, 1inch website	User	User The user is the party interacting with the DeFi protocol.
Smart Contract	The user interacts directly with the DeFi protocol using their own smart contract or a development platform. E.g.: user smart contract, Remix	User	User The user is the party interacting with the DeFi protocol.

Table 3: DeFi Protocol interface types

For interface type 'Intermediary', the KYC obligations of the user are towards the intermediary, not the DeFi protocol. This will follow traditional KYC processes such as between a user and their bank or centralized crypto exchange. That has been discussed in the original zkKYC paper [1]. If a DeFi protocol chooses to implement KYC processes, it should KYC the intermediary in this case, not the user, as it is the intermediary that interacts with the DeFi protocol. Considering the intermediary is a business, it is considered out of scope for this paper.

Oracles Specific to the DeFi context, the Holder will not only control and manage their identity related information via a self-sovereign identity (SSI) wallet, but they will also control and manage access to the private keys that control digital assets stored on the blockchain. As a result, a Holder manages two wallets: a self-sovereign identity wallet and a digital asset wallet. These wallets can be implemented separately or be merged into one. The main challenge and hence focus of the presented solution concept will be on the Verifier role and its interaction with a Holder. Due to the decentralized and permissionless nature of DeFi, along with minimised trust assumptions and the user's choice of interface to interact with a DeFi protocol, careful consideration for the appropriate approach is required.

The key responsibility of the Verifier role in zkKYC is to verify the (zero-knowledge) eligibility proofs presented by the Holder to make sure that they meet the eligibility criteria for the provided service. These criteria reflect the business requirements set out by the Verifier themselves, but also reflect regulatory requirements such as compliance with KYC obligations. In addition, the Verifier verifies the validity proof generated by the Holder, which must prove that the shared zkKYC token is valid, contains the right information and is correctly encrypted. The Verifier will store these proofs (eligibility and validity) along with the received zkKYC token (for possible future redemption if and when required). A shared characteristic of these Verifier responsibilities is that they rely on data externally provided to them. The data a Verifier must verify, is generated from verifiable credentials that reside in the Holder's SSI wallet which is stored on their device or in the cloud. DeFi protocols, however, run on public blockchains and their isolation from the external world is exactly what makes them so secure and reliable. Blockchains are designed to form consensus on the state of their shared ledger, relying on data and logic stored within it. Introducing external data to these systems and the smart contracts that run on them, requires an additional and separate piece of infrastructure, known as an oracle [15].

[1] https://app.uniswap.org

An oracle is a secure piece of middleware that facilitates communication between blockchains and any off-chain system. The ability to combine on-chain code (e.g. DeFi protocol) and off-chain infrastructure (e.g. SSI wallet) enables advanced decentralized applications that react to real-world events, incorporate off-chain data and rely on off-chain computation in a reliable and secure manner. Because the data and computation outputs delivered by oracles to blockchains directly determine the outcomes of smart contracts, it is critical that the oracle mechanism is highly reliable and secure. An oracle mechanism that relies on a single, centralized entity to deliver data to a smart contract introduces a single point of failure, defeating the entire purpose of a decentralized blockchain application. If this single entity goes offline or is corrupted, the smart contract will not have access to the (most up-to-date or accurate) data required for proper execution, or will rely on incorrect data, possibly leading to wrong outcomes. Truly overcoming the oracle problem requires decentralized oracles to prevent data manipulation, inaccuracy, and downtime [16]. In the case of zkKYC, there is only a single data source for each data element: either the Holder's SSI wallet or their digital asset wallet. Luckily, that data is under control of the Holder and it is cryptographically verifiable, so it is not possible for the Holder to provide arbitrary data. Regarding the oracle nodes, the presented solution concept suggests a Decentralized Oracle Network (DON), where multiple oracle nodes receive the data elements presented by the Holder, verify their correctness and come to a consensus on the outcome of this off-chain computation. One node then gets elected to submit this agreed upon outcome on the blockchain, as input for a DeFi protocol. Participating oracle node operators get financially rewarded for their contribution and oracle node operators that do not act honestly or reliably can be penalised or excluded from a DON. This approach minimises trust assumptions and maximises the reliability and security for communication between a Holder and a DeFi protocol. In addition, the introduction of a DON enables flexibility for the zkKYC solution concept. It makes it self-sovereign identity platform agnostic (REQ-06) by supporting multiple DID methods (and related Verifiable Data Registries) and blockchain agnostic (REQ-05) by integrating with multiple blockchains. Multiple oracle solution providers exist, each with a different approach and trade-offs. The open source oracle technology of Chainlink is considered the de facto standard for setting up a Decentralized Oracle Network, securing the majority of value locked in DeFi protocols today [17].

Reputation and Identity As the metaverse unfolds and more and more parts of life transition to on-chain applications and services, our identity and reputation will extend to this new environment. Many try to hide their real-world identity on-chain, so reputation becomes a more predominant attribute to rely upon in on-chain interactions. Someone's reputation is an opinion about that person, typically as a result of social evaluation on a set of criteria, such as behaviour or performance [18]. It's the aggregate of your behaviour over a period of time [19]. It takes time to build, but can be ruined fast. In an environment where formal structures, authorities and control are absent, reputation is critical.

One way to build reputation is via the transaction history of your digital asset wallet(s) on transparent public blockchains. It is forever auditable, an immutable track record of one's actions and performance. A digital asset wallet functions as a pseudonym, meaning that the public may know the public digital asset wallet address, but not necessarily the identity of the owner of that digital asset wallet. Anyone who is interested in a digital asset wallet can see the details of each transaction that the address has been involved in. In the context of an individual user, metrics of interest might include: total assets held, number of loans successfully repaid and number of times in default. As more and more transactions occur on public blockchains, it is hypothesised that:

- Increasingly reliable reputation scores and ratings will be calculated according to the historic transaction data of a transacting party's digital asset wallet; and
- A transacting party will easily be able to share its reputation (across one or more digital asset wallets), for example, with a transacting counterparty or regulator [20].

Another way to build reputation that is emerging, is via micro-credentials, issued and relied upon by on-chain applications and decentralized autonomous organisations (DAOs). These credentials can relate to specific events, achievements or transactions. Examples include a governance vote, the (un)staking of assets, a repayment of borrowed assets and leading a community call. Your actions become (digital) assets. Individually they might be trivial or frivolous, but in aggregate a portfolio of such credentials can represent one's identity and reputation more accurately. It can inform your credit score, your payment history, your alignment with a community or your skill level. Such micro-credentials are typically implemented as non-fungible tokens (NFTs): unique digital assets, controllable by a single individual, embedded with information about the event, achievement or transaction. Leveraging the composability, portability and interoperability of digital assets in general, they can become an important tool to signal one's reputation. A person can store them in their digital wallet, together with other digital assets and tokens. Currently they do not carry much value in the context of regulatory KYC obligations, but they can extend and enrich one's identity with valuable information to refine risk assessment. The presented approach will support such credentials and describe how and where they could fit into the overall design.

The authors point out that reputation via transaction history or micro-credentials issued on transparent public blockchains is less privacy preserving for end-users as they cannot control who consumes this information or for what purpose.

3.4 Architectural Overview

The diagram below provides an architectural overview for implementing the zkKYC solution concept in DeFi, based on the requirements, observations and design considerations outlined above. It overlays the zkKYC ecosystem model with the identified solution components that are particular to the DeFi context and their interactions. These components are described below.

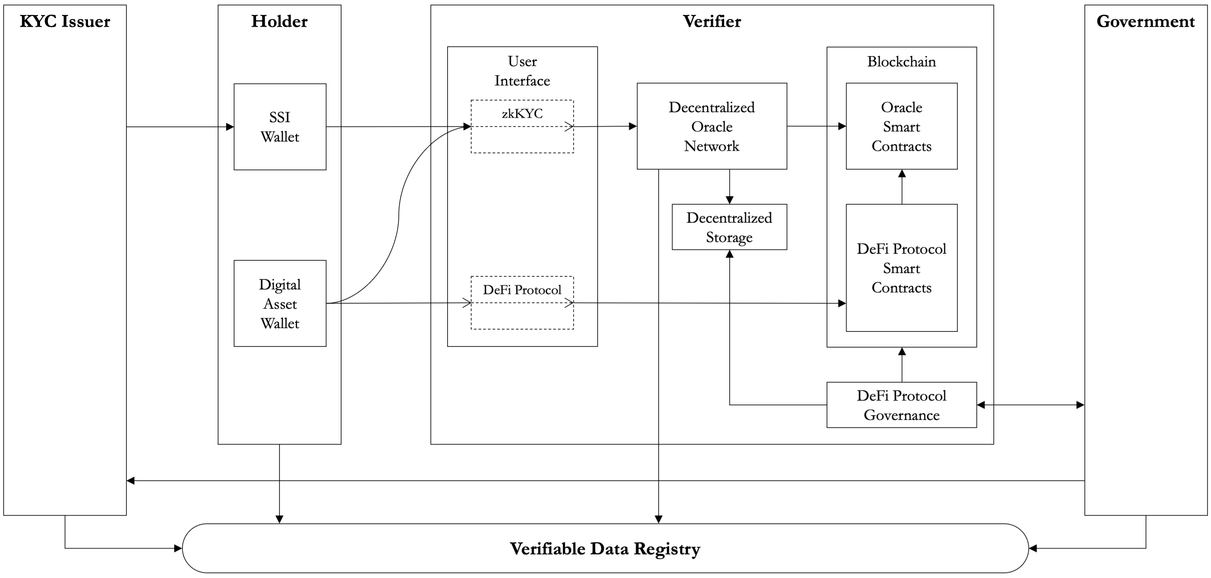

Figure 2: Architectural overview

SSI Wallet Holders store the verifiable credential issued by a KYC Issuer in their SSI wallet [21]. It reflects the outcome of their KYC process and serves as a critical element of the zkKYC solution concept. Based on this verifiable credential, the SSI wallet can generate the eligibility proofs requested by the Verifier, as well as the zkKYC token and associated validity proof.

Digital Asset Wallet The private keys associated with the Holder's digital assets are stored in their digital asset wallet. These private keys enable the Holder to control and transfer digital assets on-chain or prove they do control a particular wallet address associated with the public key. The Digital Asset Wallet may also store the private keys of any micro-credentials (as NFTs) that support the Holder's on-chain reputation.

User Interface The user interface of the Verifier is a rather abstract component. It represents the interface for a Holder and their wallets to interact with the Verifier. Functionally, this component represents a user interface for zkKYC interactions and a user interface for DeFi protocol interactions:

- zkKYC: a website or app for a Holder's SSI and digital asset wallets to interact with the DON for the purpose of zkKYC. Alternatively, this interface could also be implemented as APIs in developer SDKs or into the wallets directly.
- DeFi Protocol: a website or app for a Holder's digital asset wallet to interact with the DeFi protocol smart contracts on the blockchain. It can be implemented to access a DeFi protocol specifically (e.g. https://app.uniswap.org) or as an aggregator service (e.g. https://app.1inch.io). It can also be implemented within a development platform (e.g. Remix[2]) or block explorer (e.g. Etherscan[3]) to interact directly with the smart contracts on-chain. Last, this interface could also be implemented as a smart contract developed and deployed by the Holder, which interacts on-chain with the DeFi protocol smart contracts.

Decentralized Oracle Network (DON) The key responsibility of the DON is to provide a reliable and trusted communication bridge between the Holder and the DeFi protocol for the purpose of zkKYC. It serves as a Verifier proxy for the DeFi protocol and allows for trustless KYC verification. Based on a DeFi protocol specific configuration profile and the use case at hand, the DON interacts with the Holder's SSI wallet and issues a request for authentication or the presentation of zkKYC specific data elements including eligibility proofs, a

[2] https://remix.ethereum.org/
[3] https://etherscan.io

zkKYC token encrypted with the particular public key of Government and the associated validity proof. Each node of the oracle network will receive and verify zkKYC data from the Holder, come to consensus with the other nodes on the verification outcome and elect one oracle node to submit the outcome to the oracle smart contract on-chain. The elected oracle node is also responsible to store the relevant proofs and zkKYC token on the decentralized storage (see below). Given that the oracle network represents the DeFi protocol towards the Holder for the purpose of zkKYC, its nodes must receive delegation authority by the DeFi protocol to control its DID$_V$. This is required to establish the underlying SSI interactions with the Holder, which the oracle network is able to do given it runs off-chain.
The DON also requests proof from the Holder that they control a particular digital asset wallet. To do this, it asks the Holder to generate a digital signature using the wallet's private key that they control. Then, it cryptographically verifies whether that signature matches with the digital asset wallet's public key. The oracle nodes can perform additional verifications of the digital asset wallet such as verifying it against a black list or watch list, published by trusted authorities (see section 3.4.1 below).

Decentralized Storage Decentralized storage is used by the DON to store DeFi protocol specific configuration files as well as zkKYC verification proofs and zkKYC tokens. These Holder and DeFi protocol specific data sets must be strongly secured and guaranteed to be only accessible by authorised parties and under strict conditions. The implementation options for this component, along with possible technologies and design trade-offs, are out of scope of this paper. Options can range from a single distributed platform with advanced access rights management to DON and DeFi protocol specific platforms and technologies with standardised interfaces in order to maintain more control and sovereignty.

Oracle Smart Contracts The elected oracle node of the DON submits the outcome of the zkKYC verification to the oracle smart contracts on-chain. These smart contracts connect the DON with the DeFi protocol. The oracle smart contracts keep track via a whitelist for each DeFi protocol which of their users (i.e. DID$_{HV}$) have successfully passed zkKYC verification. Remember that DID$_{HV}$ is a unique identifier of the Holder, specific towards the DeFi protocol (i.e. Verifier). It is not re-used across Verifiers. For most blockchains, it will be linked to the digital asset wallet address of the Holder. For this reason, using different digital asset wallets across DeFi protocols will further improve user privacy.

DeFi Protocol Smart Contracts The DeFi protocol smart contracts constitute the DeFi protocol as such and are responsible for processing DeFi transactions submitted by the Holder.

DeFi Protocol Governance Each DeFi protocol that implements KYC processes is assumed to have some sort of governance entity. This can be decentralized in the form of a Decentralized Autonomous Organisation (DAO) or centralized via a traditional legal entity. The governance entity is responsible for interacting with Government and retrieving the necessary data (e.g. DID$_{HV}$, zkKYC token, transaction data) from the blockchain or decentralized storage.

3.4.1 Extensibility and flexibility

KYC Issuers, their (ongoing) customer due diligence processes, the resulting KYC credentials they issue and the SSI wallet these are stored in, are all fundamental to the implementation of zkKYC in DeFi. They focus on the real-world identity of the Holder and enable bridging the world of centralized AML/CFT regulation with the world of DeFi, while preserving user privacy. In addition, the solution architecture presented above provides the extensibility to evolve towards more decentralized forms of regulation (see section 2.2) and to enable KYC policies that include on-chain identity and reputation (see section 3.3). The DON can extend the basic zkKYC flow and rely on on-chain identity and reputation (via NFTs in the Holder's digital asset wallet) as well as consult additional data sources to enrich the verification of the Holder's identity with verification of their digital asset wallet. Examples of digital asset wallet verification sources include wallet watch lists (e.g. CipherTrace DeFi Compli[4]) and wallet risk scores by on-chain analytics companies (e.g. TRM Labs[5]).

In addition to functional extensibility, the architecture provides cross-platform flexibility. The SSI credentials can be anchored to any verifiable data registry. The digital assets that support a Holder for zkKYC can be stored on any blockchain, with no need for this to be the same blockchain as where the DeFi protocol is deployed on. This flexibility will be critical as we head towards a multi-chain future. The value of verifiable credentials and digital assets cannot be limited to or locked up in the walls of a particular registry or blockchain.

The diagram below provides an overview of how different assets in control of the Holder can provide input into the zkKYC verification process by the DON and how the DON can consult a multitude of sources to strengthen the veracity of its verification process of both SSI credentials and digital asset wallets.

[4] https://ciphertrace.com/defi-compli-sanctions-compliance-oracle/
[5] https://www.trmlabs.com/products/forensics

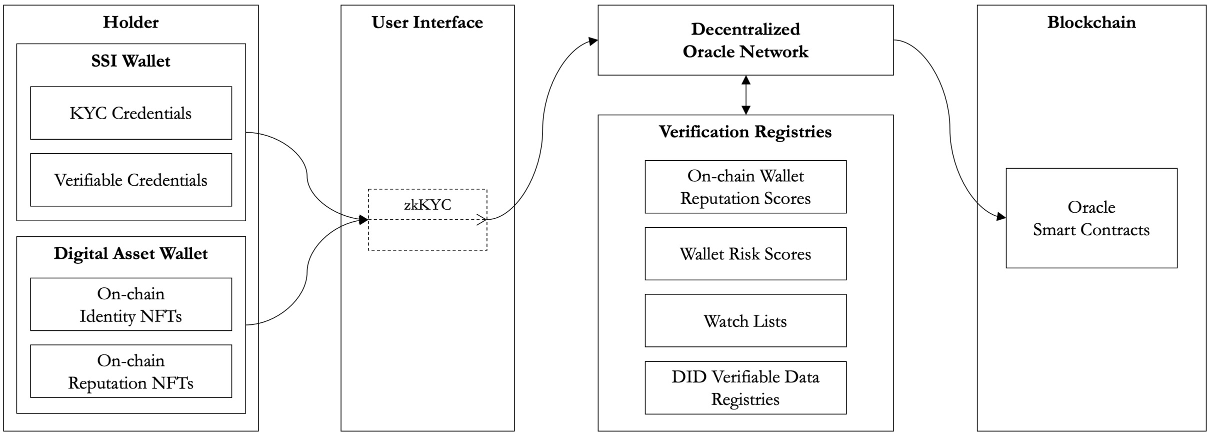

Figure 3: Extensibility and flexibility

3.5 Use Cases

The solution components presented in the architectural overview enable a number of different use cases. Additional use cases exist, but the selection presented in the diagram below supports the basic functionalities required for zkKYC in DeFi. Each use case focuses on how an actor engages with the zkKYC ecosystem to achieve a specific objective. The table below provides a high-level overview of each use case. Detailed descriptions can be found in appendix A, including how the different solution components interact to realise each use case objective.

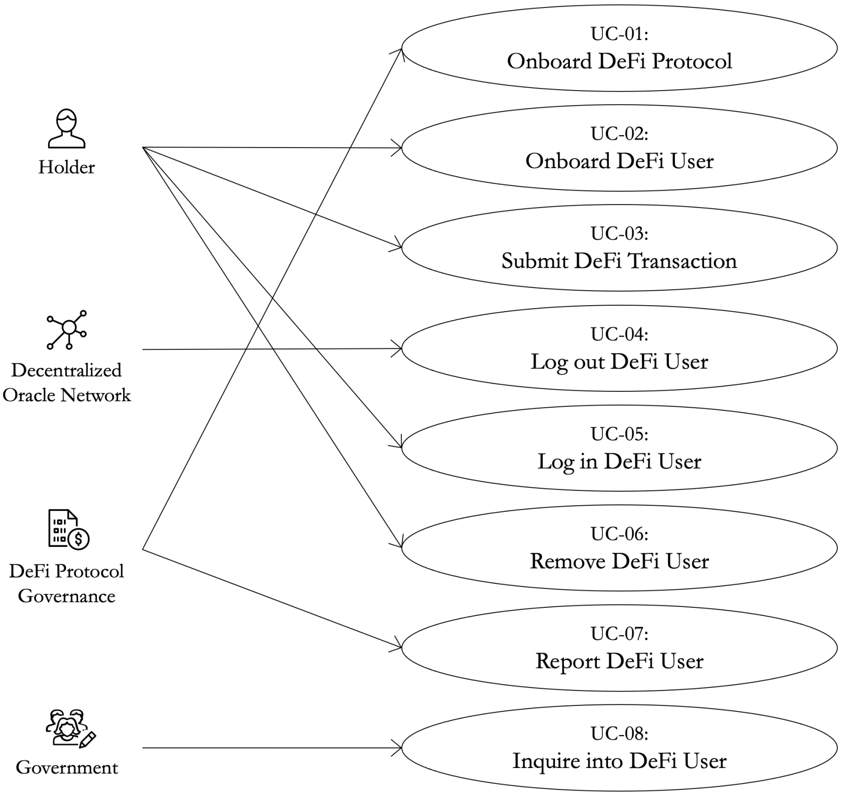

Figure 4: Use cases

ID	Use case description
UC-01	**Onboard DeFi Protocol** (see appendix A.1) The DeFi Protocol Governance team onboards the DeFi Protocol onto zkKYC. As part of the onboarding, the DeFi Protocol Governance team defines and stores configuration details in the Decentralized Storage component, accessible to the DON. Examples include decentralized identifiers, public keys, trusted KYC Issuers and requested zkKYC eligibility proofs.
UC-02	**Onboard DeFi User** (see appendix A.2) The Holder onboards themselves as DeFi User with the DeFi Protocol so they can start submitting transactions with the DeFi Protocol. As part of the onboarding, the Holder must present requested zkKYC eligibility proofs, a zkKYC token and associated validity proof. The DON performs zkKYC verification and, if successful, whitelists and "logs in" the DeFi User's Digital Asset Wallet for the DeFi Protocol.
UC-03	**Submit DeFi Transaction** (see appendix A.3) As DeFi User, the Holder submits a transaction with the DeFi Protocol. As part of the transaction processing, the DeFi Protocol verifies with the Oracle Smart Contract that the Holder's Digital Asset Wallet is whitelisted and "logged in".
UC-04	**Log out DeFi User** (see appendix A.4) As part of timely upkeep and security hygiene, and per the configuration settings of the DeFi Protocol, the DON "logs out" Digital Asset Wallets that have been whitelisted for the DeFi Protocol.
UC-05	**Log in DeFi User** (see appendix A.5) Once logged out, the Holder logs in their Digital Asset Wallet that has already been whitelisted for the DeFi Protocol. This occasion is an opportunity for the DON to perform zkKYC verification as part of ongoing customer due diligence, per the configuration of the DeFi Protocol.
UC-06	**Remove DeFi User** (see appendix A.6) The Holder removes their Digital Asset Wallet from a DeFi Protocol's whitelist. Holders might do this because they do no longer use the DeFi Protocol or their Digital Asset Wallet, or as security measure because their Digital Asset Wallet was lost, hacked or stolen. Upon authentication, the DON removes the Digital Asset Wallet from the whitelist.
UC-07	**Report DeFi User** (see appendix A.7) The DeFi Protocol Governance team reports a Digital Asset Wallet to Government because of an adversarial situation (e.g. hack or theft of funds), suspicion of fraud, money laundering or other criminal activity. They retrieve the DeFi User's zkKYC token and hand it over to Government who can reveal the DeFi User's identity by decrypting the token, identifying the relevant KYC Issuer and requesting them the identity information they need about the DeFi User.
UC-08	**Inquire into DeFi User** (see appendix A.8) Government asks a DeFi Protocol to provide the zkKYC token of a particular DeFi User (via their Digital Asset Wallet) based on identified criminal behaviour, in order to reveal their identity. Using the zkKYC token, Government can identify the relevant KYC Issuer and ask them the information about the Holder they need.

Table 4: Use cases

3.6 Conclusion

The unique nature of DeFi protocols and the platforms they operate on has surfaced a list of additional requirements for any solution approach that aims to implement zkKYC in DeFi without compromising any of the core values that underpin them. Built on top of the design considerations regarding KYC Issuers, flexible user interface support and DONs to establish on-chain truth about off-chain entities, this section has presented a solution approach that implements zkKYC in DeFi in alignment with its values and unique nature. A list of detailed use cases describes the different scenarios in a DeFi User's life cycle and how the identified solution components interact to realise each use case. The next section focuses on how this ecosystem of a diverse set of actors can be governed and incentivised to grow and operate successfully.

4 Ecosystem

In a business context, an ecosystem can be described as an economic community supported by a foundation of interacting organizations and individuals – the organisms of the business world. This community comprises a multilateral set of participants who are aligned and incentivized to interact in order to co-create value [22]. These participants take up one or more defined ecosystem roles and thereby pursue distinctive interests, provide unique contributions and bring their own expectations to their involvement in the ecosystem. The zkKYC ecosystem as presented in sections 3.1 and 3.4 supports this definition. This section presents zkKYC ecosystem governance, suggests a commercial model for incentive alignment and explores how to bootstrap and spur adoption of a 'zkKYC in DeFi' ecosystem.

4.1 Governance

Ecosystem governance is the system by which ecosystem participants and their resources are directed to realise the ecosystem's purpose. It is concerned with structure and processes for decision making, accountability, control, interactions and behaviour. Governance influences how objectives are set and achieved, how risk is monitored and addressed and how performance is optimised. In the context of zkKYC in DeFi, the following (non-exhaustive) elements are considered in scope of ecosystem governance:

- Supported KYC policies (see section 2.2);
- Compliance with specific jurisdictional AML/CFT regulations;
- Standards regarding KYC Credentials issued by KYC Issuers (e.g. data elements and structure);
- Supported DID methods (and Verifiable Data Registries);
- Incentive mechanism and commercial model (including liability regime);
- Selection criteria, review mechanisms and integration processes for the onboarding of ecosystem participants including KYC Issuers, DeFi Protocols, DON, SSI wallets, digital asset wallets and user interfaces;
- Decision making process;
- Disagreement and dispute resolution process;
- Ongoing ecosystem architecture and design.

AML/CFT regulations differ across jurisdictions. It is therefore a relevant consideration whether the scope of a zkKYC solution implementation and its ecosystem governance should be specific to a single jurisdiction, span multiple jurisdictions (e.g. regional) or be global (in line with the nature and objective of DeFi protocols). All options are technically possible and the objective is of course to pursue a global zkKYC ecosystem.

Whether we talk about enterprises, nation states or DeFi protocols, governance in general has been a much-debated topic in recent years. The emergence of DAOs as a vehicle for the governance of DeFi protocols (and other collective endeavours) has created a renewed focus on the following dimension of governance; centralized vs. decentralized. This provides the following options for setting up ecosystem governance for zkKYC in DeFi:

- **Centralized**: a single, closed entity has full control over the creation, roll-out and governance of an ecosystem (and possibly a specific zkKYC solution implementation). This option can improve the speed of decision making and roll-out into the market, but might be harder to spur adoption and get broader support, especially given the decentralized spirit of DeFi protocols.
- **Governance Council**: a single entity that has representation from a set of key ecosystem participants. Decision making happens centrally, via a consensus mechanism (e.g. majority voting) amongst the representatives. This option can include dedicated (sub-)committees that focus on a particular topic (e.g. technology, commercial model). This model is widely used in enterprise consortia and provides a compromise between central control and ecosystem representation. A challenge is to secure representation from a diverse set of participants, not limited to the largest players or those with the biggest (financial) interests.
- **DAO**: an emergent form of organisational structure whereby governance is decentralized and encoded in one or more smart contracts on a public blockchain. DAOs allow a vast and widely distributed set of participants (including individuals, companies and other DAOs) to coordinate their decision-making and resources transparently [23]. While this new form of governance has garnered strong appeal as a response to the perceived perils of centralized governance, it also inhibits risks and challenges due to its young history and evolving nature. Much is still to be discovered, learned and improved. The authors also note that there is to date no precedent of a DAO that would govern the development of a solution and ecosystem with the regulatory focus (i.e. AML/CFT) that zkKYC has. Aspiring to do this from the outset as a DAO, publicly and permissionlessly, is a major challenge. There are however different options to give birth to a DAO: "DAO First" vs. "Exit to DAO" [24]. DAO First refers to choosing for a DAO-based approach from the start of a project, including the initial rules of token distribution and capital formation. The alternative to a DAO First approach is progressive decentralization where projects build out their solution, ecosystem

and community using centralized governance in order to "exit to a DAO" over time, i.e. "decentralize" decision making power to the ecosystem community. This approach can be found with DeFi protocols such as Compound or Uniswap where development of a product version (and funding for that) is centralized, but the post-release governance is handed over to a DAO.

The governance options for both jurisdictional scope and level of (de)centralization can receive a different preference as the zkKYC ecosystem evolves and adoption increases.

4.2 Commercial Model

Sustainable ecosystem design includes incentive models to stimulate participation and "desirable behaviour" in order to co-create value for the entire ecosystem, while maintaining competitive behaviour. To date, blockchain based protocols (including DeFi protocols) have incorporated mechanisms for incentive alignment and distribution of rights and obligations in a variety of innovative ways, including via (value accruing) cryptographic tokens, address specific rights or other means.

Principles The proposed arrangement of incentivisation for the zkKYC ecosystem participants is based on the following basic principles:

- The participants that create, verify or share valuable information are rewarded for their value creation. This includes at least:
  - The KYC Issuers, for performing the (ongoing) KYC verification process and issuing and revoking verifiable KYC credentials accordingly;
  - The DON, for performing the zkKYC verification in name of the DeFi protocols;
  - The ecosystem governance entity, i.e. zkKYC Governance Body, for their governance activities.
- The participants that rely on the outcome of the zkKYC verification (i.e. DeFi protocols) pay for the consumed information and services rendered to them as it provides them regulatory compliance (in case of AML/CFT) and risk mitigation in general (by deterring bad actors and behaviour).
- Holders are shielded as much as possible from financial transactions related to zkKYC.

These principles are quite straightforward and unsurprisingly similar to what can be found in Digital Identity or Credit Card Payment schemes: the issuer and scheme owner get paid, the relying party pays.

Commercial model Applying these principles to a zkKYC commercial model looks as follows:

- A DeFi protocol pays the zkKYC Governance Body when onboarding at the zkKYC ecosystem (see UC-01). This can be a one-time payment or a periodic subscription. The zkKYC Governance Body can use this to pay for internal expenses and to fund ecosystem development. In case the zkKYC Governance Body is implemented as a DAO, this payment could return governance tokens to the DeFi protocol so it can actively participate in future ecosystem governance.
- A DeFi protocol pays each time a Holder onboards themselves (see UC-02) or authenticates themselves (see UC-05). As these use cases are initiated by the Holder, a debit-type payment transaction is preferred. It is suggested that the DeFi protocol pre-funds a smart contract controlled by the DON or the zkKYC Governance Body for these payments. As a minimum balance threshold is crossed, an event can be issued so that DeFi Protocol Governance can replenish the smart contract funds. An automated DON Keeper job can distribute these payments at set intervals using a predefined distribution key to the following entities:
  - The contributing DON oracle node operators. The DON report that is submitted on-chain to onboard or authenticate a user includes digital signatures of the participating oracle node operators which can be used to identify and pay them. Operators are paid for running the oracle network, verifying zkKYC presentations and possibly paying data sources (e.g. wallet risk scoring providers, watch lists) for access.
  - The KYC Issuer that issued the verifiable credential used by the Holder. The KYC Issuer's DID_I points to a DID Document in the Verifiable Data Registry in which a service endpoint for payments can be configured. This can include a digital asset wallet of the KYC Issuer where payments can be made into. As KYC Issuers are responsible for verifying a Holder's identity, performing ongoing customer due diligence and issuing and revoking verifiable credentials accordingly, their payment is critical to a healthy zkKYC ecosystem.
- Reporting a DeFi User (see UC-07) or inquiring into a DeFi User (see UC-08) does not incur any specific costs. It is considered part of the DeFi Protocol Governance operations and responsibilities.

The authors suggest that the above payments are made using digital assets, given the nature of DeFi protocols and the infrastructure they run on. These digital assets could be existing tokens (e.g. existing oracle network tokens, stablecoins) or a new token specific to the zkKYC ecosystem. This decision is up to zkKYC ecosystem governance. Fiat payments are harder to coordinate, are more expensive to process and take longer to settle across multiple jurisdictions. There are of course opportunities for service providers to offer easy fiat on- and off-ramps.

Liability An essential component of the zkKYC ecosystem governance is the definition of a liability regime. Who bears accountability when things go wrong? From a regulatory perspective, the regulated entity (i.e. the DeFi protocol) is liable for meeting their obligations. However, from a zkKYC ecosystem perspective it makes sense to be able to hold KYC Issuers and data sources (e.g. watch lists) accountable for the provision of incorrect information (due to not adhering to defined processes) or for their failure to appropriately and timely update KYC information. They are compensated for providing exactly this service to the highest quality standards. Therefore, we can anticipate that any possibilities for recourse should be incorporated into the zkKYC commercial model. While further details are out of scope of this paper, it would be neglectful not to mention that liability is a complex matter and requires sufficient attention as part of the ecosystem governance.

4.3 Adoption

Building out a (global) zkKYC in DeFi ecosystem and creating network effects within that ecosystem takes time. It is expected that the trend towards self-regulation in addition to laws and regulations relating to KYC (particularly AML/CFT) in certain jurisdictions will spur demand (from DeFi Protocols and those who seek to integrate DeFi protocols) for a system which facilitates KYC policies for DeFi protocols. Early movers for KYC in DeFi have already been sighted [25], [26], [27]. Initial adoption by DeFi protocols can be further incentivised by granting ecosystem governance rights or (temporarily) improved commercial terms. The paragraphs below focus on SSI wallets, KYC Issuers, scalable interoperability and Government to spur adoption in the wider ecosystem.

SSI and SSI wallets are a fundamental building block of the zkKYC solution concept, but their adoption is currently rather limited. Where adoption exists, it is mostly in context of a use case or geography specific ecosystem. zkKYC, using a generic KYC credential, has the potential to scale their usage across many verifiers and use cases. A condition is that zkKYC capabilities are built into these wallets. Short-term focus on the development of an open-source SDK that can be embedded in these SSI wallets is therefore required. Prominent SSI wallet providers such as Spruce, Trinsic, MATTR and Evernym are prime candidates. Alternatively, SSI and zkKYC capabilities could be built as an addition to already popular digital asset wallets (e.g. MetaMask - particularly given its ability to integrate plug-ins [28]), but this might be a more challenging option given the technology and domain specific knowledge required.

The initial KYC Issuers will play an important role in the adoption of zkKYC. Globally active centralized exchanges (such as Coinbase, Kraken, FTX and Gemini) are extremely well positioned due to their existing KYC policies across many jurisdictions for a wide set of users and their experience in and knowledge of the blockchain industry and DeFi protocols in general. Issuing KYC credentials to their customers can help these exchanges generate an additional source of income and build a competitive advantage over other exchanges in attracting new customers. Over the longer term, retail banks (e.g. Commonwealth Bank of Australia [4]) will become well suited as well given their existing customer base who have already been KYC'd and their increasing appetite towards blockchain-based products.

To maximize adoption and usability, the authors believe the zkKYC solution should be open sourced and designed and built such that the same system can easily be coded in multiple languages and used across multiple blockchains (Layer 1 and Layer 2). A blockchain agnostic and open-source DON will greatly contribute to this goal. This approach will also improve the scalability of the zkKYC ecosystem and the interoperability across blockchain platforms and DeFi protocols.

Those parties that currently enforce legislation and (AML/CFT) regulation in each of the jurisdictions that zkKYC aspires to operate, are best positioned to fulfill the zkKYC ecosystem role of Government. It is however a reasonable expectation that they will not be able to take up this role from the start. This can be due to technical reasons (e.g. controlling a self-sovereign decentralized identifier and associated cryptographic keys) or due to reasonable prudence regarding engaging in such a novel approach and young ecosystem. In this scenario one or more entities acting as Government must emerge to effectively "self-regulate" the zkKYC ecosystem. A zkKYC Governance Body is a primary candidate to take up this role at the start, on the condition it implements appropriate processes and controls for access to sensitive, personal information about Holders in the ecosystem.

5 Conclusion

A comparison between the worlds of AML/CFT regulation and DeFi can be characterised as a clash of cultures on several topics: the level of centralisation, permissionless nature, privacy, sovereignty, trust assumptions. It is evident that imposing "as-is" KYC processes to DeFi protocols is impossible due to the decentralized, trust-minimised and transparent nature of blockchains. Personal identifiable information cannot be shared with on-chain applications and linking personal identifiable information with digital asset wallets risks unintended consequences for the privacy and safety of the individual. In this paper, the authors have presented an approach to apply the zkKYC solution concept to DeFi. The zkKYC solution concept is extended with the introduction of KYC Issuers and Decentralized Oracle Networks (DONs) as key solution components. This approach upholds the zkKYC premise of simultaneously providing regulatory transparency as well as fully protecting an individual's privacy. KYC Issuers verify the identity of an individual, but have no knowledge about their digital asset wallets or DeFi activity. DeFi protocols interact with digital asset wallets, but have no knowledge about the identity of the individual controlling them. If and when deemed necessary, only a designated governance entity is able to reveal the identity of an individual that is under strong suspicion of being a bad actor in a DeFi protocol. The proposed solution architecture supports ongoing customer due diligence, blockchain agnosticism, and configurability per the requirements of each DeFi protocol and their jurisdictional AML/CFT obligations. It provides extensibility towards future on-chain identity and reputation systems and flexibility in supporting verifiable credentials anchored in any registry and digital assets stored on any blockchain. The paper has presented how all roles and solution components interact to realise the identified requirements and a list of use cases without enforcing any implementation decisions or technology choices. Last, the authors have explored considerations regarding governance, commercial model and adoption in order to achieve a healthy and sustainable 'zkKYC in DeFi' ecosystem.

5.1 Further Considerations

Alternative Applications The problem statement of this paper put the focus on KYC policies for the purpose of regulatory compliance (AML/CFT). A solution concept has been presented to implement zkKYC in DeFi and achieve regulatory compliance to the extent that requirements to do so can be assumed to be known at this stage. The benefit of demonstrating the ability to meet strict regulatory requirements is that it enables also additional applications for zkKYC in DeFi, including customer eligibility policies and operational risk management. Below a few examples:

- DAOs could benefit from zkKYC to establish membership eligibility criteria based on off-chain identity attributes.
- On-chain applications could allow access to their services based on (off-chain) proof of residency in specific jurisdictions rather than relying on IP addresses which can be easily bypassed using VPNs.
- Decentralized lending protocols could rely on off-chain credit scores or proof of liquidity in order to grant under-collateralized loans.

Know-Your-Business (KYB) The zkKYC solution concept has focused on individuals as customers, not businesses. In the case of businesses, KYC is also often called Know-Your-Business (KYB). zkKYC could also be applied to KYB. There might be less private and sensitive information required to establish the identity of a business, much of the information is also public, but it is often much more complex. Regulatory requirements for businesses can be stricter and more diverse across jurisdictions and industries. Also, the legal construction of a business can be quite complicated, along with the financial ties and interests. As a result, a KYB process can often take many times longer (and cost many times more) than the KYC process of a retail individual.

The role of a KYC Issuer (or KYB Issuer in this case) for zkKYC in DeFi serves the specific context of KYB very well. KYB Issuers specialise in customer due diligence of businesses of which the outcome can then be re-used by the business towards DeFi protocols. Business banks (e.g. Silvergate Bank) are prime candidates to take up this role of a KYB Issuer. We see an early version of this concept with Aave ARC who will rely on institutional custodian Fireblocks and their KYB processes to whitelist businesses to Aave ARC's permissioned lending/borrowing pools [25]. In this specific example it is a formal business agreement between Aave and Fireblocks, but this could be opened up, with a business more in control, using zkKYC. As with zkKYC for individuals, it evidently requires proper ecosystem governance and clarifications on legal, commercial and liability implications as well as business and technical standardisation of credentials and identity verification processes.

A key benefit of zkKYC for businesses, and improvement over the approach with Aave ARC and Fireblocks, is that the KYB Issuer must not be aware of the Digital Asset Wallet of the business and their DeFi transactions. The business can keep their transactions more private (e.g. via self-custody or custody at another entity than the KYB Issuer) while ensuring compliance with regulatory KYB obligations as expected by institutional DeFi protocols.

Trust DeFi protocols and the blockchains they run on are often called trustless because, as a user, you are not required to trust a particular entity. Even more, every change in the system is verifiable and a decentralized network of nodes verify each other's actions to hold each other accountable. This trustless nature is key to the DeFi value proposition. This is why reliance on external, off-chain data was initially looked upon critically, as it assumed the need to trust that data and the party that put it on-chain. Luckily, the oracle problem has been addressed by specialised protocols via DONs that can bring off-chain data on-chain in a reliable and secure manner, ready to be used by DeFi protocols. In the case of zkKYC, however, there is admittedly still a source of trust required: trust in the KYC Issuer. The KYC Issuer performs the KYC processes to identify an individual and issue a KYC verifiable credential that the individual, as Holder, can subsequently use in a zkKYC ecosystem. This approach puts trust in the KYC Issuer. They must be highly specialised, professional and rigorous. As mentioned earlier in the paper, this creates a risk of the centralisation of power and gatekeeping and that is why a large and diverse set of KYC Issuers is required. A proper commercial model for zkKYC can help to mitigate this risk. In the longer term, we can anticipate zkKYC, even for the purpose of regulatory compliance, becomes more driven by on-chain identity and reputation. Together with improved cross-chain interoperability, this will contribute to further minimising the trust assumptions.

5.2 Next Steps

Valuable feedback on the original zkKYC paper from regulators and subject matter experts has been instrumental in informing the authors of the requirements for zkKYC in DeFi. The requirement of ongoing customer due diligence, even in the context of DeFi, to enable regulatory compliance is a good illustration of this. Therefore, the review by and constructive feedback from subject matter experts along with open discussions and suggestions to further improve the solution concept for zkKYC in DeFi is highly welcome. The more this concept is challenged and tested, the better and more complete it has the opportunity to become.

A particular topic that warrants further research and discussion is the definition of what constitutes ”strong suspicion of being a bad actor in a DeFi protocol” as a trigger for a designated governance entity to be able to request the identity of a DeFi user to be revealed. Even if such governance entity is in fact a collection of entities, possibly organized as a DAO, where no single centralized entity can initiate this process unilaterally (e.g. via threshold encryption), it warrants clarity on a clear definition of the conditions that must be met for a DeFi user's identity to be revealed.

In addition, the authors encourage anyone who is interested to implement this solution concept in a prototype and share their findings and feedback. Designing and implementing the zero-knowledge proving system for zkKYC tokens is a valuable challenge to tackle. Not just must it work functionally, but it should also achieve a performance cost for generating the proof that is acceptable from a user experience perspective. Proof size and verification time is probably less of an issue given it happens off-chain.

Acknowledgements

This paper builds on top of the initial zkKYC paper, but would not have been possible without the endless amount of inspirational people, communities, papers, articles, podcasts, tweets and even memes out there. They have triggered reflections, ideas, challenges and confirmations that would not have surfaced otherwise. This serves a reminder how far this space has come thanks to collaboration, open debate and the sharing of ideas and feedback.

The authors also want to acknowledge the many people that have provided feedback on the initial zkKYC paper. Whether it were technical questions, risk observations or regulatory considerations, they have played a role in shaping the concepts presented in this paper. Thank you.

Last but not least, a lot of gratitude and recognition goes towards subject matter experts Michael Mosier, Juan Caballero, JP Koning and Jake Chervinsky for their thorough review and valuable feedback, and towards Sagit Shiran for tirelessly revising and proofreading. Their insightful comments and suggestions have improved the quality of this paper. Thank you.

References

[1] Pieter Pauwels. *zkKYC: A solution concept for KYC without knowing your customer, leveraging self-sovereign identity and zero-knowledge proofs.* June 2021. URL: https://ia.cr/2021/907.

[2] Defi Llama. *Ethereum Total Value Locked.* Jan. 2022. URL: https://defillama.com/chain/Ethereum.

[3] Dune Analytics. *Total DeFi users over time.* Jan. 2022. URL: https://dune.xyz/queries/2972.

[4] Commonwealth Bank of Australia. *CBA to offer crypto services to customers.* Nov. 2021. URL: https://www.commbank.com.au/articles/newsroom/2021/11/CBA-to-offer-crypto-services.html.

[5] Dr. Tom Robinson and Chris DePow. *DeFi: Risk, Regulation, and the Rise of DeCrime.* Elliptic. Nov. 2021. URL: https://www.elliptic.co/resources/defi-risk-regulation-and-the-rise-of-decrime.

[6] Investopedia. *Financial Technology – FinTech.* July 2020. URL: https://www.investopedia.com/terms/f/fintech.asp.

[7] Finematics. *What is DeFi? Decentralized Finance Explained (Ethereum, MakerDao, Compound, Uniswap, Kyber).* July 2020. URL: https://finematics.com/defi-explained/.

[8] Aave. *Flash Loans - Pushing the limits of DeFi.* 2021. URL: https://aave.com/flash-loans/.

[9] AUSTRAC. *AML/CTF programs overview.* Aug. 2020. URL: https://www.austrac.gov.au/business/how-comply-guidance-and-resources/amlctf-programs/amlctf-programs-overview.

[10] Dr. Tom Robinson. *Bitcoin Blockchain Analysis & DOJ Indictment of Russian Hackers.* Elliptic. July 2018. URL: https://www.elliptic.co/blog/doj-indictment-russian-hackers-blockchain-analysis.

[11] Wolfie Zhao. *Poly Network attacker returns $256 million of the stolen cryptocurrency.* The Block. Aug. 2021. URL: https://www.theblockcrypto.com/post/114189/poly-hack-attacker-return-funds-id-slowmist.

[12] Balaji S. Srinivasan. *#259 - The reckoning to come: a conversation with Balaji Srinivasan.* Making Sense podcast by Sam Harris. Sept. 2021. URL: https://www.samharris.org/podcasts/making-sense-episodes/259-reckoning-come.

[13] Wikipedia. *Nothing to hide argument.* Nov. 2021. URL: https://en.wikipedia.org/wiki/Nothing_to_hide_argument.

[14] Hayden Adams. Uniswap. July 2021. URL: https://twitter.com/haydenzadams/status/1418961999539712006.

[15] *What Is the Blockchain Oracle Problem?* Chainlink. Aug. 2020. URL: https://blog.chain.link/what-is-the-blockchain-oracle-problem/.

[16] *What Is a Blockchain Oracle?* Chainlink. Sept. 2021. URL: https://chain.link/education/blockchain-oracles.

[17] *Total Value Secured All Oracles.* Defi Llama. Jan. 2021. URL: https://defillama.com/oracles.

[18] Wikipedia. *Reputation.* Dec. 2021. URL: https://en.wikipedia.org/wiki/Reputation.

[19] Andrew Beal. *30,000 Feet - Issue #40: Micro-credentials & Web3 Reputation.* Oct. 2021. URL: https://30000feet.substack.com/p/issue-40-micro-credentials-and-web3.

[20] James Olsen. *Relative Performance Ranking: Reputation Score Model Proposal.* MyCelium Research, Reputation, Nov. 2021. URL: https://static.reputation.link/whitepapers/RPR_Whitepaper.pdf.

[21] Anna Johnson. *Trinsic Basics: What Are SSI Digital Wallets?* Trinsic. Aug. 2020. URL: https://trinsic.id/what-are-ssi-digital-wallets/.

[22] Michael Hilb. *From Corporate to Ecosystem Governance.* Board Perspectives. Oct. 2021. URL: https://www.boardperspectives.com/post/from-corporate-to-ecosystem-governance.

[23] Jack Deeb. *DAOs and Australia.* Nov. 2021. URL: https://mirror.xyz/deeb.eth/9LrgMv8gNpcijk90qV4Es-DeURVbJjVY8knoEc1a1yM.

[24] Kelsie Nabben. *Experiments in algorithmic governance continue. Trying not to fail at Decentralised Autonomous Organisations (DAOs).* July 2021. URL: https://kelsienabben.substack.com/p/experiments-in-algorithmic-governance.

[25] Aave. *Introducing Aave Arc.* Nov. 2021. URL: https://aave.mirror.xyz/JcA9DzQHK6o8YYMmxtH43Vqq5HoHvjrTrFnd_UprKWQ.

[26] TBD54566975. *Introducing tbDEX.* Nov. 2021. URL: https://tbd54566975.ghost.io/introducing-tbdex.

[27] Centre. *Verite: Decentralized identity for crypto finance.* Feb. 2022. URL: https://www.centre.io/verite.

[28] Dan Finlay. *Introducing Web3 Plugins.* MetaMask. Oct. 2019. URL: https://medium.com/metamask/introducing-the-next-evolution-of-the-web3-wallet-4abdf801a4ee.

A Appendix: Use Cases

A.1 UC-01: Onboard DeFi Protocol

Actor	DeFi Protocol Governance
Objective	Onboard the DeFi Protocol onto zkKYC so that Holders can start using zkKYC as DeFi Users.
Preconditions	None
Steps	The DeFi Protocol Governance team defines and stores the following information elements, in requested format, in the Decentralized Storage component: • **DeFi protocol's Smart Contract address** that will interact with the Oracle Smart Contract. • **DeFi protocol's Decentralized Identifier** (DID_V). The associated encryption keys must be delegated and be controllable by the node operators of the DON (possibly via threshold encryption). • **zkKYC eligibility proofs** that the DeFi Protocol requires from its users. Examples include: – minimum age – residency of a particular jurisdiction – minimum level of assurance for identification – sanctions lists that the user has been verified against by the KYC Issuer – issuance date of KYC credential – VDR published revocation lists that should be verified against • **Wallet Screening lists** at a Holder's Digital Asset Wallet should be verified against. This can include: – Watchlists and blacklists (e.g. OFAC) – On-chain transaction monitoring service provider that issues risk scores to Digital Asset Wallets (e.g. Chainalysis, CipherTrace, TRM Labs ...) – Any other type of metric regarding a Digital Asset Wallet • List of **trusted KYC Issuers**, using their decentralized identifiers (i.e. DID_I). Only eligibility proofs and zkKYC tokens generated based on verifiable credentials from those KYC Issuers will be accepted. • **Government public key(s)** that the Holder must use to encrypt the zkKYC token with. There could be multiple public keys (for multiple parties taking up the Government role) or there can be a single public key together with a threshold encryption scheme, so any or a particular number of Government parties can decrypt it. • **DON Keeper configuration details** for logging out whitelisted DeFi Users. This includes the time period after which logged in whitelisted DeFi Users must be logged out.
Notes	The zkKYC eligibility proofs mentioned above rely on off-chain credentials, as per the zkKYC model. These eligibility proofs could be extended to include on-chain (micro) credentials that are stored in the Holder's Digital Asset Wallet and inform a Holder's on-chain reputation.

Table 5: UC-01: Onboard DeFi Protocol.

A.2 UC-02: Onboard DeFi User

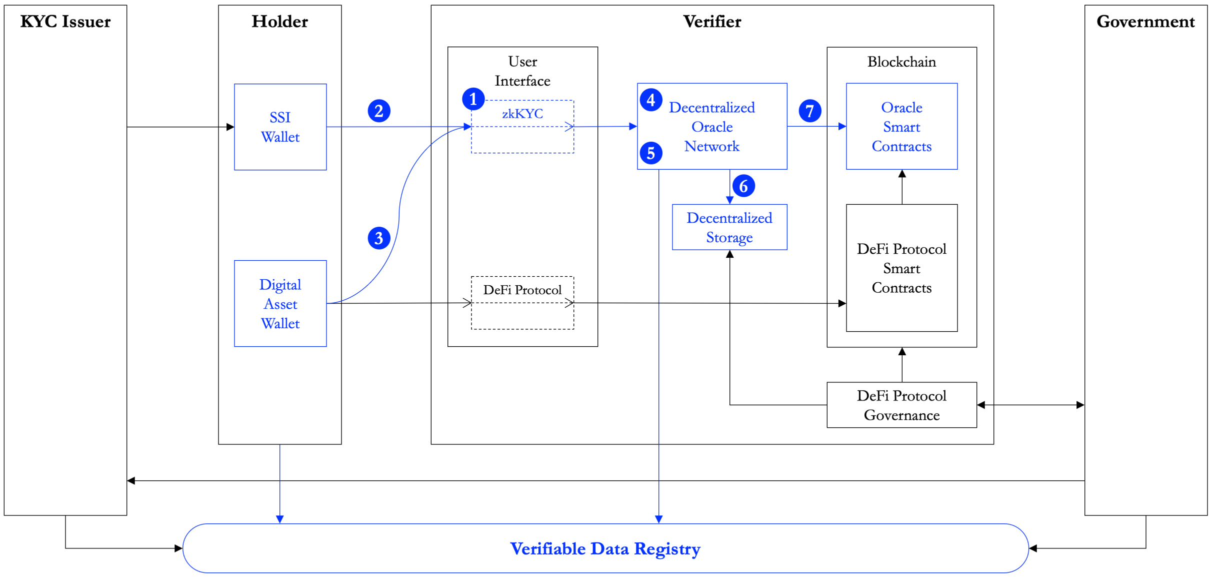

Figure 5: UC-02: Onboard DeFi User

Actor	Holder
Objective	Onboard the Holder as DeFi User with the DeFi Protocol so they can start submitting transactions with the DeFi Protocol.
Preconditions	UC-01
Steps	Onboarding a DeFi User follows the following steps: 1. Holder selects a zkKYC User Interface to onboard with the DeFi Protocol. This interface provides the capability for the Holder to connect their SSI Wallet and Digital Asset Wallet. Behind the User Interface is the DON, which the Holder actually interacts with to onboard as DeFi User at the selected DeFi Protocol. 2. Holder uses their SSI Wallet to generate a DID$_{HV}$ (unique and specific to DID$_{V}$; the DeFi Protocol) and establishes a secure (SSI) relationship with DID$_{V}$. The DON controls DID$_{V}$ (representing the DeFi Protocol) because the DeFi Protocol itself cannot control private keys. This step authenticates Holder towards DID$_{V}$ by proving control over DID$_{HV}$. 3. Holder proves control over their Digital Asset Wallet (i.e. address) to the zkKYC DON. To do this, the Holder generates a digital signature using their wallet's private key. Then, the DON cryptographically verifies whether that signature matches with the digital asset wallet's public key. 4. The DON verifies whether the Holder's Digital Asset Wallet has not been published on any blacklist or watchlist (e.g. OFAC). The lists to verify against, if any, are specified by the DeFi Protocol as part of its onboarding. 5. Holder completes zkKYC verification. This includes presenting requested zkKYC eligibility proofs and generating a Verifier specific zkKYC token as well as associated validity proof. As part of this activity, the DON also verifies that the KYC credential (VC) used by the Holder has not been revoked by the KYC Issuer. It does this by checking against a revocation list/accumulator on the Verifiable Data Registry (VDR).

	If zkKYC verification is successful and all DON nodes come to consensus on this outcome, then the DON elects one oracle node to: 6. Store DID_{HV}, DID_{V}, the zkKYC token and the current timestamp in the Decentralized Storage, all encrypted so that only the DeFi Protocol Governance can decrypt it. Further on-boarding information could be stored as well such as the KYC Issuer (DID_{I}). 7. Submit an oracle report to the Oracle Smart Contracts, which whitelists the Holder's Digital Asset Wallet address to the DeFi Protocol, associates it with DID_{HV} and DID_{V} and marks it as "logged in". The Holder is now onboarded as DeFi User with the DeFi Protocol. If zkKYC verification is not successful, then the Holder will not be onboarded.
Notes	The zkKYC verification checks outlined above can easily be extended to include verification of on-chain (micro) credentials that are stored in the Holder's Digital Asset Wallet and verification of on-chain wallet reputation that could be stored on-chain and don't require verification against off-chain sources (see REQ-09). To minimize trust assumptions even further, it is possible to implement the verification logic of the DON in this use case as a provable off-chain computation for which a zero-knowledge proof could be submitted on-chain and verified for correct execution. There are hopeful developments to realise this goal with provable programming languages such as Cairo (by StarkWare) and Leo (by Aleo), but consider this out of scope for the focus of this paper.

Table 6: UC-02: Onboard DeFi User.

A.3 UC-03: Submit DeFi Transaction

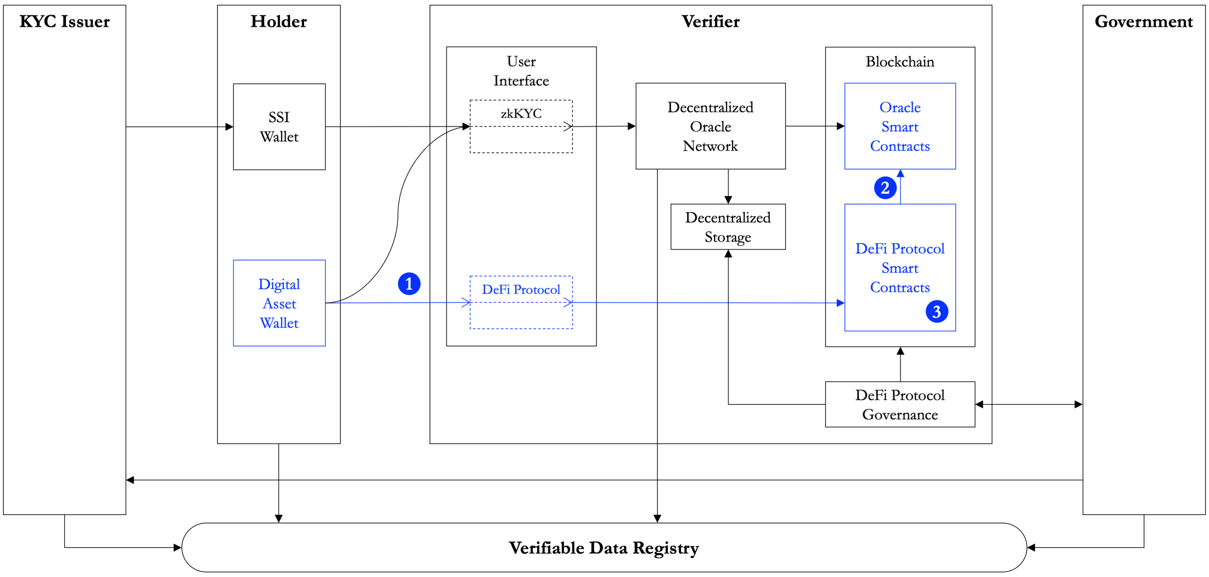

Figure 6: UC-03: Submit DeFi Transaction

Actor	Holder
Objective	Submit transactions to the DeFi Protocol for execution
Preconditions	UC-02
Steps	Submitting transactions to the DeFi Protocol follows the following steps: 1. Holder selects a DeFi Protocol User Interface of choice to submit a DeFi Transaction using their Digital Asset Wallet to sign the transaction. 2. The DeFi Protocol Smart Contracts validate if the transaction sender (wallet address) is whitelisted for their protocol and "logged in" by calling upon the Oracle Smart Contract and passing DID_V and the DeFi User's wallet address. 3. The DeFi Protocol Smart Contracts execute based on the response of the Oracle Smart Contract: (a) If the DeFi User's wallet is whitelisted for the calling DeFi Protocol Smart Contract and "logged in", then the submitted DeFi transaction is executed. (b) If the DeFi User's wallet is not whitelisted for the calling DeFi Protocol Smart Contract, then the submitted DeFi transaction is not executed and the user is directed to UC-02. (c) If the DeFi User's wallet is whitelisted for the calling DeFi Protocol Smart Contract but "logged out", then the submitted DeFi transaction is not executed and the user is directed to UC-04.

Notes	To prevent rejected DeFi transactions due to the DeFi User's wallet not being whitelisted or being "logged out" (see UC-04), the Holder could check the status of their wallet for a particular DeFi Protocol with the Oracle Smart Contract off-chain prior to submitting a transaction to the DeFi Protocol. Such capability could be implemented in the DeFi Protocol User Interface, improving the user experience and saving on unnecessary gas costs. The additional effort for existing DeFi Protocol Smart Contracts to integrate zkKYC is minimal. A few additional lines of code can conditionally execute existing transaction processing logic based on the outcome of an Oracle Smart Contract function call. To support future privacy preserving DeFi Protocols (see REQ-12), it should be assumed that the Digital Asset Wallet is not known to the DeFi Protocol, or at least not stored on-chain along the transaction data. In this case, the Holder's wallet address cannot be associated with a whitelisted Holder identifier (DID_{HV}) in the Oracle Smart Contract. To bypass this limitation, the DeFi Protocol must require the Holder to pass along DID_{HV} with the DeFi Transaction data. This can then be verified (in zero-knowledge) against the Oracle Smart Contract for being whitelisted towards the DeFi Protocol. Note that this would require more impactful changes to the smart contract and zero-knowledge proving logic of these DeFi Protocols, but there are possibilities to achieve this if desired.

Table 7: UC-03: Submit DeFi Transaction.

A.4 UC-04: Log out DeFi User

Actor	Decentralized Oracle Network
Objective	Log out a DeFi User's Digital Asset Wallet that has been whitelisted for the DeFi Protocol as part of timely upkeep and security hygiene.
Preconditions	UC-02
Steps	As part of a fully decentralized and trustless approach towards DevOps and upkeep, the DON provides off-chain computation capabilities that can trigger on-chain smart contract execution based on predefined criteria. For security reasons it is not desirable that DeFi users stay "logged in" for a long time period. For the sake of an optimal user experience, it is not desirable for a DeFi User to have to authenticate themselves via their SSI Wallet every time they want to submit a DeFi transaction. It is up to each DeFi Protocol Governance team to define a compromise by configuring a time period after which each whitelisted DeFi User of their DeFi Protocol gets "logged out" and must re-authenticate themselves via their SSI Wallet before being able to submit a DeFi transaction again. This time period is driven by the security vs. user experience trade-off of the DeFi Protocol. At the frequency of block creation, the DON checks the Oracle Smart Contracts for "logged in" whitelisted Digital Asset Wallets that have to be "logged out" based on the configuration of the DeFi Protocols for which they have been whitelisted. Remember that a Digital Asset Wallet must be whitelisted for each DeFi Protocol separately. The DON could also take into account the most recent on-chain activity of a particular Digital Asset Wallet with the DeFi Protocol. This way, inactive wallets are logged out quickly, but wallets that are active in the DeFi Protocol remain logged in for a longer time.
Notes	While the focus of this use case is on security, it could also be applied for regulatory compliance reasons to support Ongoing Customer Due Diligence. See UC-05 for more details.

Table 8: UC-04: Log out DeFi User.

A.5 UC-05: Log in DeFi User

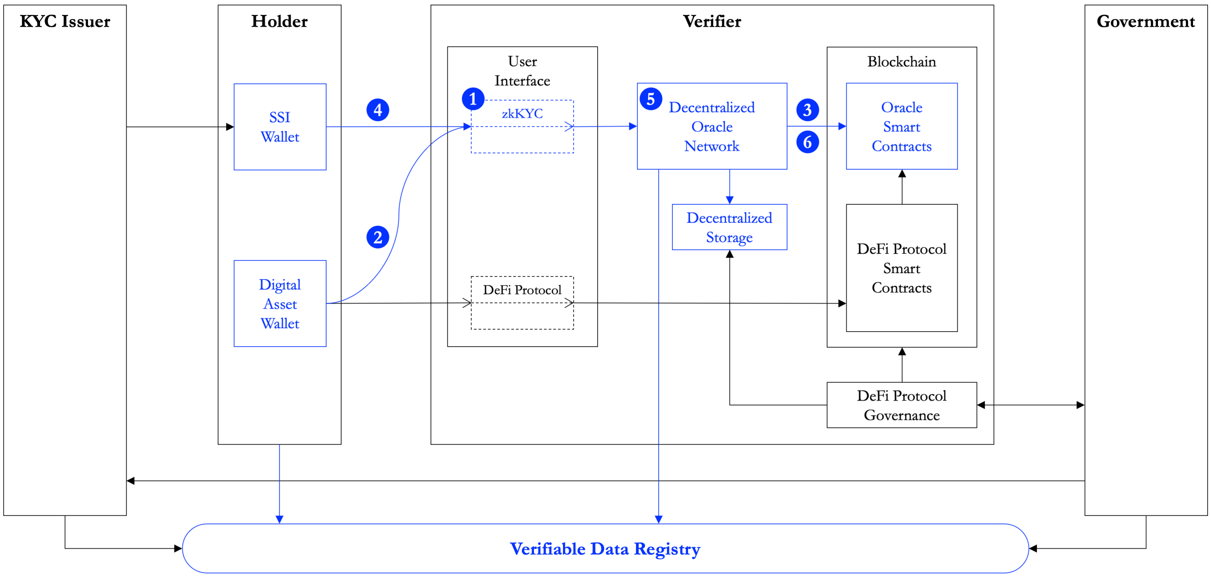

Figure 7: UC-05: Log in DeFi User

Actor	Holder
Objective	Log in a DeFi User's Digital Asset Wallet that has already been whitelisted for the DeFi Protocol
Preconditions	UC-04
Steps	Logging in a DeFi User follows the following steps: 1. Holder selects a zkKYC User Interface to log in and authenticate themselves as a DeFi User for the DeFi Protocol (DID$_V$). This interface provides the capability for the Holder to connect both their SSI Wallet and Digital Asset Wallet. 2. Holder proves control over their Digital Asset Wallet (i.e. address) to the zkKYC DON. To do this, the Holder generates a digital signature using their wallet's private key. Then, the DON cryptographically verifies whether that signature matches with the digital asset wallet's public key. 3. The DON looks up the verified Digital Asset Wallet in the Oracle Smart Contract and verifies that it has been whitelisted for the DeFi Protocol (DID$_V$) and has been logged out. If confirmed, the DON retrieves the associated DID$_{HV}$ and returns it to the zkKYC User Interface. 4. The Holder is asked to prove control over DID$_{HV}$ by signing a challenge using the private key associated with DID$_{HV}$. This step authenticates Holder towards DID$_V$ by proving control over DID$_{HV}$. 5. Before logging in the DeFi User's Digital Asset Wallet on-chain, the DON has the opportunity to introduce additional verifications as part of Ongoing Customer Due Diligence. Based on DeFi Protocol specific configuration, this step allows the DON to: (a) Verify that the KYC credential (VC) used by the Holder has not been revoked by the KYC Issuer by checking it against a revocation list/accumulator on the Verifiable Data Registry (VDR). (b) Request the Holder to generate updated Eligibility Proofs. (c) Request the Holder to generate a new zkKYC token (and associated Validity Proof).

	5. (d) (Re)verify whether the Holder's Digital Asset Wallet has been published on any blacklist or watchlist (e.g. OFAC). (e) (Re)verify whether the Holder's Digital Asset Wallet risk score at an on-chain transaction monitoring service provider is acceptable. (f) (Re)verify any other type of metric regarding the Holder or their Digital Asset Wallet. 6. If any introduced re-verifications are successful and related proofs stored on Decentralized Storage, the elected oracle node submits an oracle report to the Oracle Smart Contract, which updates the whitelisted Holder's Digital Asset Wallet address to the DeFi Protocol to "logged in". The Holder is now re-authenticated as DeFi User with the DeFi Protocol and can submit transactions again.
Notes	The verification checks as outlined in step 5(f) above can include verification of on-chain (micro) credentials that are stored in the Holder's Digital Asset Wallet and verification of on-chain wallet reputation that could be stored on-chain and don't require verification against off-chain sources (see REQ-09).

Table 9: UC-05: Log in DeFi User.

A.6 UC-06: Remove DeFi User

Actor	Holder
Objective	Remove a DeFi User's Digital Asset Wallet from a DeFi Protocol's whitelist. Holder's motivations to do this include: • DeFi User does not use the DeFi Protocol anymore. • DeFi User does not use Digital Asset Wallet anymore. • DeFi User implements security measures because Digital Asset Wallet was lost, hacked or stolen.
Preconditions	UC-02
Steps	Removing a DeFi User follows the following steps: 1. Holder selects a zkKYC User Interface to remove their Digital Asset Wallet from the DeFi Protocol's (DID$_V$) whitelist. This interface provides the capability for the Holder to connect their SSI Wallet. 2. Holder proves control over DID$_{HV}$ by signing a challenge using the private key associated with DID$_{HV}$. This authenticates the Holder towards DID$_V$ by proving control over DID$_{HV}$. 3. The DON looks up the authenticated DID$_{HV}$ in the Oracle Smart Contract and verifies that it has been whitelisted for the DeFi Protocol (DID$_V$). If confirmed, the DON retrieves the associated Digital Asset Wallet(s) and presents it to the Holder in the zkKYC User Interface. 4. Holder selects the Digital Asset Wallet(s) they want to remove. 5. The DON elects an oracle node to submit an oracle report to the Oracle Smart Contract, which removes the selected DeFi User's Digital Asset Wallet address(es) from the DeFi Protocol whitelist.

Table 10: UC-06: Remove DeFi User.

A.7 UC-07: Report DeFi User

Actor	DeFi Protocol Governance
Objective	Report a DeFi User to Government because of an adversarial situation (e.g. hack, theft of funds), suspicion of fraud, money laundering or other criminal activity.
Preconditions	UC-03
Steps	Reporting a DeFi User follows the following steps: 1. DeFi Protocol Governance identifies one of their DeFi Users to meet the protocol's criteria to be reported to Government for formal investigation. This decision can be informed by on-chain transaction behaviour of the Digital Asset Wallet. Several organisations have already emerged who provide on-chain analytics services (e.g. Reputation, Chainalysis, TRM Labs). 2. Using the DeFi User's Digital Asset Wallet's address along with the DeFi Protocol's DID (DID$_{V}$), the associated Holder identifier (DID$_{HV}$) can be retrieved from the Oracle Smart Contract. 3. DeFi Protocol Governance is authorised to retrieve the zkKYC token associated with DID$_{HV}$ and DID$_{V}$ from the Decentralized Storage. They decrypt the outer encryption layer, so the zkKYC token can be shared with Government. 4. DeFi Protocol Governance shares the zkKYC token associated with the DeFi User with Government, along with the Digital Asset Wallet address, DID$_{HV}$, DID$_{V}$ and any relevant transaction information that supports their claims and can help Government's investigation. 5. Government reviews the shared information. If identification of the associated individual is required, Government can decrypt the zkKYC token using their private key and verify that it contains the correct Holder identifier (DID$_{HV}$) and the correct Verifier identifier (DID$_{V}$). The token will also reveal a KYC Issuer identifier (DID$_{I}$) and associated Holder identifier (DID$_{HI}$) of whom they want to reveal the true identity. Government contacts the identified KYC Issuer using service endpoints specified in the DID Documents of their resolved DID$_{V}$. The KYC Issuer is asked to provide personal information about the associated Holder identifier in the token (i.e. DID$_{HI}$). Considering the KYC credential was issued by this KYC Issuer, they must have successfully verified the identity of this Holder. This verified identity information can now be used by Government to identify the Holder and pursue their investigation.
Notes	It is important to note that it requires multiple steps and decisions by multiple actors for a particular DeFi User's identity to be revealed: 1. DeFi Protocol Governance must agree to retrieve and decrypt zkKYC token. Often this governance is decentralized and a decision to do so requires a majority vote. 2. DeFi Protocol Governance shares information with Government. 3. Government decrypts zkKYC token. This can be set up with a threshold encryption system to avoid one individual or entity can complete this step. 4. Government must reach out to the relevant KYC Issuer who must then agree to share requested information to reveal an identity to Government. This approach enables identity revelation where required while avoiding surveillance at scale.

Table 11: UC-07: Report DeFi User.

A.8 UC-08: Inquire into DeFi User

Actor	Government
Objective	Inquire into a particular DeFi User of a DeFi Protocol in order to reveal the identity behind the pseudonym.
Preconditions	UC-03
Steps	Inquiring into a particular DeFi User follows the following steps: 1. As part of a (broader) ongoing investigation, Government is interested in a particular DeFi User. This interest can be driven by identified suspicious or criminal behaviour patterns by the DeFi User's Digital Asset Wallet at the DeFi Protocol itself (DID_V) or at another DeFi Protocol. 2. Government reaches out to the DeFi Protocol Governance with the DeFi User's Digital Asset Wallet address. Government requests DeFi Protocol Governance to share the associated zkKYC token, along with DID_{HV}, DID_V and any relevant transaction information. 3. DeFi Protocol Governance uses the received Digital Asset Wallet's address along with the DeFi Protocol's DID (DID_V) to retrieve the associated Holder identifier (DID_{HV}) from the Oracle Smart Contract. 4. DeFi Protocol Governance is authorised to retrieve the zkKYC token associated with DID_{HV} and DID_V from the Decentralized Storage. They decrypt the outer encryption layer using their private key, so the zkKYC token can be shared with Government. 5. DeFi Protocol Governance shares the zkKYC token associated with the DeFi User with Government, along with DID_{HV}, DID_V and any relevant transaction information requested by Government. 6. Government reviews the received information. Government can decrypt the zkKYC token using their private key and verify that it contains the correct Holder identifier (DID_{HV}) and the correct Verifier identifier (DID_V). The zkKYC token will also reveal a KYC Issuer identifier (DID_I) and associated Holder identifier (DID_{HI}) of whom they want to reveal the true identity. Government contacts the identified KYC Issuer using service endpoints specified in the DID Documents of their resolved DID_V. The KYC Issuer is asked to provide personal information about the associated Holder identifier in the token (i.e. DID_{HI}). Considering the KYC credential was issued by this KYC Issuer, they must have successfully verified the identity of this Holder. This verified identity information can now be used by Government to identify the Holder and pursue their investigation.
Notes	It is important to note that it requires multiple steps and decisions by multiple actors for a particular DeFi User's identity to be revealed. See UC-07 for more details.

Table 12: UC-08: Inquire into DeFi User.