ONCHAINID

Whitepaper v1.0 PUBLIC

ONCHAINID

The identity system for compliant digital assets

ONCHAINID is a blockchain-based identity ecosystem that identifies individuals and organisations, allowing them to enforce compliance and access digital assets

onchainid.com

Executive summary

ONCHAINID is an identity system that allows users to create and manage **self-sovereign identities on the blockchain**. This identification solution allows the enforcement of regulatory legal and other compliance processes and rules regarding digital assets, and enforcement of such processes and rules on any web-based system that requires identity validation.

The main added value of ONCHAINID is that it enables **compliance and identity verifications within the pseudonymous framework of public blockchain networks.**

The ONCHAINID protocol is already used by securities issuers and financial institutions to automate the validation of compliance rules in connection with security token transactions[1]. As the blockchain industry matures, its application across economic activities broadens and accelerates. **The ONCHAINID protocol can be used for permissioned "Decentralised Finance" or "DeFi", bringing the compliance layer currently missing for the institutional players to step in.** In addition to personal data, it can also be used to represent the identification data of virtually anything (real estate, art, financial assets, connected objects, etc). Coupled with other blockchain systems such as the T-REX protocol for permissioned tokens, it allows for the recovery of crypto-currencies such as Bitcoin, or stablecoins like USDC and DAI. Finally, it allows for a universal log-in system controlled by its owner.

To interact with the ONCHAINID smart contracts deployed on the blockchain, **web applications are provided to allow users to control their identity**: consult their data, request data access from other users, grant access to specific data to other users, add/modify data linked to their ONCHAINID, manage one or several wallets associated to their identity, and participate in the governance of the ONCHAINID ecosystem.

In order to reach critical mass of users and partners as quickly as possible, Tokeny, the company that initiated the ONCHAINID system, has decided to open up the governance of the protocol by issuing **OID, a governance token to incentivise the various players in the value chain and accelerate the decentralisation of the ecosystem**. OID tokens allow holders to participate in the governance of ONCHAINID and interact more broadly with the protocol, its applications, and its participants. Numerous entities such as securities issuers, investors, auditors, governmental entities, large financial institutions, custody solutions and law firms have already accepted to join the ONCHAINID ecosystem.

[1] More information available on Tokeny's website: https://tokeny.com/onchainid/

Decentralised identities: the compliance bridge between TradFi and DeFi

Decentralised Finance, or DeFi, is a blockchain-based form of finance that does not rely on central financial intermediaries and instead utilizes smart contracts deployed on blockchains. Today, DeFi is at a crossroads: The explosive growth of the industry in the recent past suggests that it fulfills a real and large demand from end users. However, its future growth beyond the crypto sphere depends entirely on its ability to attract a wider range of investors, and in particular large financial institutions.

Self-sovereign -or Digital- identity solutions and, more broadly, the ability to enforce, manage and control critical compliance rules on public blockchains is the missing link that will drive the institutional adoption of public blockchains, unleash the potential of DeFi and enable regulators to ensure the fairness, freedom and security of the Internet of Value for the benefit of all stakeholders.

DeFi needs institutions

Decentralised finance is only in its infancy. Its potential is impossible to anticipate, as it comprises the whole finance industry and the way in which value is perceived. **To grow, DeFi needs to have more value (money and assets) in circulation and be leveraged in all the innovative smart contracts** that are allowing the automation of financial services, such as onchain lending or automated market making.

DeFi has already portrayed the power that decentralised systems can have in reducing the number of intermediaries in the financial sector. Protocols like Compound, AAVE or Uniswap have enabled **models that were previously unthinkable,** and have seen their TVL ("Total Value Locked") grow exponentially, reaching billions of dollars in just a few months.

Unfortunately, **decentralised finance is still a dangerous environment for its users**. It is often difficult for investors to understand the technical fundamentals of protocols and, above all, there is **no control over the different stakeholders as everything is anonymous**: It is generally very complicated to know who deployed a smart contract on the blockchain as wallets can be generated very easily and frequently. It is also almost impossible to know who the other protocol users are. Smart contracts create and execute trust between participants thanks to coded rules that are triggered by users. But this is not enough to guarantee the protection of users in the event of theft, bank run, scam, poor workmanship, etc.

Financial institutions can help DeFi take it to the next level by bringing stability and **becoming the trusted entities necessary for the proper functioning of the ecosystem**. They have a track record in respect of distribution and investment volumes, but also, and more importantly, a set of good practices to promote the **growth of the financial system while protecting its participants**. This growth will primarily come from the volumes brought by financial institutions, but also from the role of trust they can take to bring legitimacy to DeFi. Of course, it will be necessary for the fundamentals of DeFi to persist and not to re-intermediate the system with players who are omnipresent in the ecosystem.

Institutions need compliance

In order to enter the ecosystem, and integrate their customers and networks, **financial institutions must be able to apply the compliance rules that they are subject to,** which aim to protect their customers and prevent the financing of illicit activities and other misdeeds.

Although blockchain inherently brings many guarantees by providing a resilient and secure infrastructure that allows for the transfer of value at a lower cost, **it is essential to regulate such infrastructure to be able to know who is responsible for what in the value chain**.

> For this, it is necessary to have an identity system making it possible to represent the stakeholders onchain, and validate their eligibility in accordance with applicable regulations without revealing their identities to all participants.

Permissioned DeFi protocols

Currently, one of the main applications of DeFi is the lending and borrowing of crypto-assets. Thanks to blockchain protocols, users interact not with a known intermediary, but with a series of smart contracts that will aggregate supply and demand and carry out the operations necessary for the proper functioning of the system (collateralisation, liquidations, etc.).

In comparison with comparable activities (when they exist) in more traditional finance, these protocols remove a certain number of intermediaries from the equation, reduce risks and greatly accelerate the speed of exchanges. However, **as users' direct interaction is with smart contracts, it is no longer possible, or at best extremely complicated, to know with whom they interact indirectly**: Who has deployed the smart contracts that I use, who are the other users, are these parties reliable? These issues prevent institutional investors from joining DeFi because they cannot ensure compliance with applicable regulations (AML, etc.) intended to protect investors.

Institutional participants do not necessarily need to know all the information relating to all participants of a DeFi protocol in order to be compliant, but they would need, for example, to be sure that other participants are only from a defined list of countries, are not appearing in terrorist lists, whether they are individuals with capacity to act or they are legal entities. Also, and most importantly, they need to **make sure that the protocol creator/deployer/operator has been verified and identified by a trusted party** (connection with the national digital identity, signatures from an auditor or a Know Your Customer ("**KYC**") agent, etc.)

In order to attract these institutional participants, DeFi protocol operators could duplicate their smart contracts and launch several versions restricted to different types of users, like AAVE with AAVE Arc, but it would certainly be more **pertinent to use an onchain identity system allowing programmatically to assess the eligibility of a user for a given protocol.** It would enable Permissioned DeFI in a flexible way.

Permissioned tokens

One of the key features to such an adoption from institutions is to support a framework for the **issuance, distribution and management of tokenised financial instruments** allowing those institutional stakeholders to fulfil their **regulatory obligations in terms of compliance, KYC and AML regulations and reporting**. In short, an issuer of a financial instrument deployed on a blockchain infrastructure needs to be able to guarantee that, at any time, they know who holds a position in their tokens and that such holders are "compliant" from a regulatory perspective.

In view of such regulatory constraints, **it is not possible to have such tokenised financial instruments held through unidentified wallets.** The wallets need to be associated with onchain identities, allowing access to the data of the holders to be able to assess whether they are "eligible" to hold and transact in a certain token from a regulatory standpoint.

Obviously, this does not mean that data associated with identities would be visible and accessible to anyone, as such data would only be visible and accessible to relevant parties for the purpose of fulfilling their regulatory obligations. **The control of the identity holder's digital identity and access to its related data should always remain with the identity holder,** in order to comply with data protection regulations (e.g. the General Data Protection Regulation ("**GDPR**") in Europe).

Such a framework is needed to support the deployment and holding of financial instruments on public blockchains by and for institutions. As DeFi continues to develop, regulatory obligations have started, and will continue, to apply to DeFi actors and their ability to comply with such regulations will be paramount to the further and wider adoption of DeFi by institutional investors to become mainstream.

Users need self-sovereign identities

On the Internet that we use every day to consult, create and exchange information, our **identities are mainly managed with email accounts**, usually provided by Google, Microsoft, Apple or other organisations. On the internet of value, the blockchain, we can hopefully do better and make a self-sovereign identity system the market standard.

During the last decade, data privacy has been a subject of concern for a lot of people, as the current way of processing and storing private data, as well as the procedures to erase all traces of private data on the web, is opaque and subject to **many violations of privacy**. GDPR and other regulations are trying somehow to give back control of their data to users. With the blockchain, we now have the opportunity of doing things differently: It is possible to create **a digital passport, under the control of its owner**, issued on an immutable and resilient infrastructure, adaptable to contain all kinds of proof of identity.

It is currently very easy to log in on decentralised applications ("**DApps**") with a wallet, in a few clicks and without giving passwords to any website. However, most wallets are not connected to any verified account and **prevent users from accessing financial instruments such as tokenised securities and to legally prove the ownership of their assets**. To get a verified blockchain account, users must use centralised platforms such as exchanges. However, as a consequence they get a centralised service with a mutualised wallet, not a segregated one. What if users could link their self-custody wallets to their own blockchain profile, and decide who can access their data?

As digital assets become democratised, they also become institutionalised. This means that regulations are gradually becoming more complex, not to block the evolution of the blockchain, but to protect its users. In traditional finance, the answer to complex regulations is usually to define strict criteria that service providers must follow in order to be authorised to transact on behalf of their clients. On the blockchain, technically, end-users can manage their account on their own (custody, transfers, etc.). However, **most people want safeguards, without giving up control of their data.** Scams, loss of keys, rapid technological developments and other issues show that end users need assistance to use blockchain safely. It will take more safeguard before most people start contracting decentralised home loans. Could we get the safety of a centralised service, with the control of a decentralised one?

The recent approach of some regulators has been to consider the wallet as a bank account. However, a wallet is more of a browser than an account. It is necessary to add an identity layer above the wallets, a blockchain account, which would make it possible to **manage several blockchains, several digital assets, distributed in several wallets, while keeping onchain proofs of ownership**.

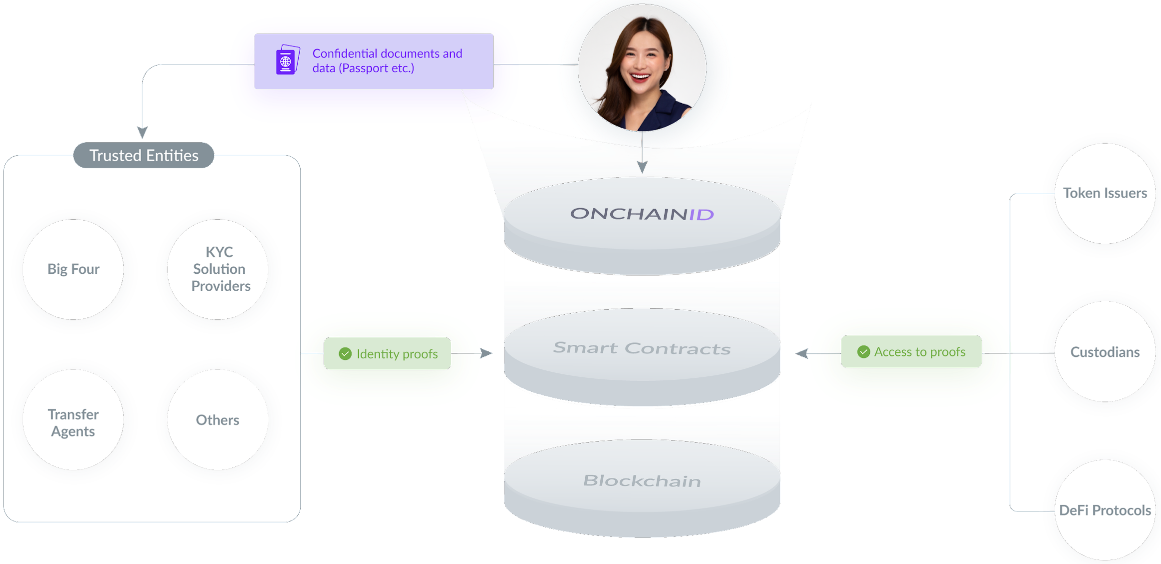
What is the ONCHAINID protocol?

Main concept

The ONCHAINID protocol is a set of smart contracts (based on ERC734-735) and applications to represent individuals, companies, programs, objects and other types of assets on the blockchain. This allows them to be identified digitally and to assign them rights, duties or simply information, over a decentralised infrastructure.

ONCHAINID **self-sovereign identities** are stored on the Polygon network, in a decentralised way. They could easily be deployed on any EVM (Ethereum Virtual Machine) compatible blockchain network. They can't be hidden or deleted. No service or organisation can remove its owner access rights to it, and it spans a lifetime.

Yet, an Identity has no value itself. **It is the information (claims) attached to it that gives credit to the identity.** This information can be self-attested, or signed on the blockchain by a trusted third-party such as a bank, a digital national identity key, a digital asset marketplace, a transfer agent, an auditor, etc. Such trusted third-parties create identity proofs that can be used by token issuers, custodians, DeFi protocols, etc.



Of course, **sensitive private information would not be stored publicly on the blockchain**. The Claim Issuer stores the claim private data on secure off-chain servers, and decides to **publish publicly on-chain a signature by a trusted third-party attesting the data**

verification. Therefore, everyone knows that a trusted third party has successfully checked the identity. But to access the data, one would need the explicit consent of the *Identity Owner* allowing the consultation of such private data. If the signature attesting the proof of identity is not issued by a credible entity in the opinion of someone who needs the relevant data, it would be possible for such person to do its own checks directly with the identity owner, as the identity owner can share the relevant information with any person by giving them simple access to its ONCHAINID.

Therefore, ONCHAINID allows identity owners to aggregate their information and certifications on a single onchain identity, while maintaining decentralisation of the data storage.

As a result, ONCHAINID enables **anonymous credentials**, it allows onchain compliant pseudonymity:

Anonymous	**Pseudonymous**	**Public**
Actual status of blockchain	ONCHAINID	Not acceptable in blockchain
Users are free to manually or automatically create wallets. Access is controlled by digital keys which can be exchanged, lost or stolen. It is not possible to guarantee on the blockchain who is the holder of the wallet and the tokens and rights that it holds. If the wallet address is technically a pseudonym, users can change easily and manage many in parallel, making it difficult to create a unified identity profile. While wallets can have been whitelisted (potentially by many parties), there is no evidence of its whitelisting/acceptance on the blockchain.	Each user controls its own identity smart contract in which they can manage their personal information, link one or more wallets, and give access to all or part of their information to trusted third parties. Directly on the blockchain, it is possible to guarantee the ownership of wallets, data and assets. Users use their pseudonym (ONCHAINID address and/or ENS) to identify themselves and prove through blockchain evidence that they are eligible to use permissioned protocols or permissioned tokens.	Identity information is obviously confidential and publicly revealing it can create significant identity theft problems. This is especially the case on the blockchain where most applications concern the transfer of value and management of assets.

In short, ONCHAINID is:

- A self-sovereign identity system
- An aggregator of certified information
- A smart contract under the control of the Identity owner
- A compliance layer preserving confidentiality
- A universal login for the internets
- A cross-chain, multi-wallets and multi-assets management system
- Viable for individuals, companies, assets, protocols and things

The ONCHAINID system was originally designed as an integral part of **the T-REX Protocol, allowing the issuance, management and transfer of permissioned tokens**: The issuer of the token acts as a trusted entity for its token holders. It is mostly used for security tokens, payment ecosystems and loyalty programs.

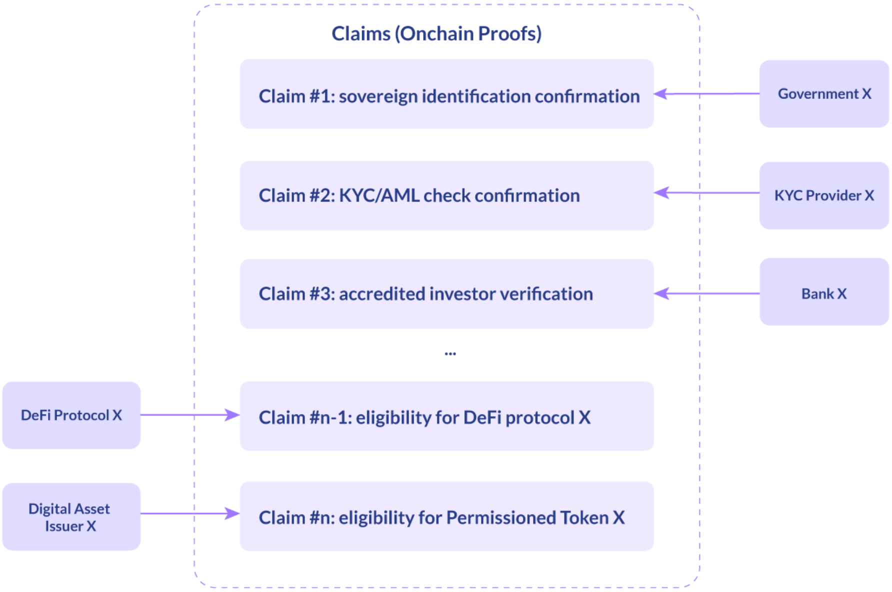
T-REX is based on the creation and the use of digital identities securely and immutably created and maintained on the blockchain infrastructure on behalf of all parties to a subscription and transactional process in security tokens (issuer, KYC provider, security token administrative agent and obviously, investors) or, more broadly, permissioned tokens issued under the protocol [2] .

In particular, with regards to investors, those identities allow them to securely (hashed) maintain on the blockchain either information or, more generally, links to information about themselves that they can, ***under their own control***, make available to 3rd parties (a KYC provider, a website in which they want to login, authorities, …) on request.

Most interestingly, **it allows accredited parties - Trusted Claims Issuers - to add qualifying information to an identity** (e.g. a KYC provider having checked an investor and attaching to the investor identity a "statement" that such investor qualifies for holding and transacting in a certain security token; a marketplace operator adding a claim to an investor identity reflecting that such investor has been duly checked and admitted as an investor on that marketplace, ...). Note that, in fine, **it is always the *identity owner* who will decide whether or not a claim is added to his/her identity**.

[2] While T-REX has been initially designed to support the issuance of security tokens, Tokeny has seen various use-cases for issuing permissioned tokens under the protocol which are not necessarily financial instruments: e.g. loyalty programs tokens, stablecoins for a use in specific ecosystem, immobilised crypto-currencies, etc...

ONCHAINID Claims
(Individual/Corporate)


Claims (Onchain Proofs)
Claim #1: sovereign identification confirmation
Government X
Claim #2: KYC/AML check confirmation
KYC Provider X
Claim #3: accredited investor verification
Bank X
...
DeFi Protocol X
Claim #n-1: eligibility for DeFi protocol X
Digital Asset Issuer X
Claim #n: eligibility for Permissioned Token X

Tokeny, the software company developing the T-REX protocol, has developed all the ONCHAINID tools allowing not only to create identities on behalf of various stakeholders as part of an investment process in a permissioned token, but also to create identities independently of such a process. The status on these developments is as follows:

- The smart contracts to be used for identity management on the blockchain (based on the ERC734[3]/735[4] standards) are in production and used both on Ethereum and on Polygon;

- Documentations, APIs (Application Programming Interfaces) and SDKs (Software Development Kits) in terms of how to use and populate these identities (in particular for trusted third parties) are final and available to the ONCHAINID community;

- Interfaces needed to create and administer the identities, as part or independently of a token subscription process, have been rolled out and will be further developed going forward.

The management of digital identities has the potential to support all activities on Blockchain requiring onchain permissioning and automated compliance.

[3] https://github.com/ethereum/eips/issues/734
[4] https://github.com/ethereum/eips/issues/735

How do ONCHAINIDs work ?

ℹ️ *For detailed information, please visit docs.onchainid.com*

How to get and manage an ONCHAINID

Concretely, ONCHAINID identities are Smart Contracts, deployed on the blockchain. **Users can get their own identity by using the ONCHAINID web app, or by following the onboarding process of a compatible DeFi protocol, security token issuer or digital asset marketplace.**

The user provides its information and documents depending on the use case and automatically obtains its ONCHAINID smart contract with signed certifications on the blockchain. Technically, this smart contract is deployed by the ONCHAINID software, and then the management keys are given to the main wallet of the identity owner. The identity can then be enriched and evolve according to the needs of the user and the applications it uses. Other wallets can be connected to the Identity and the identity owner can decide which one(s) has a management key.

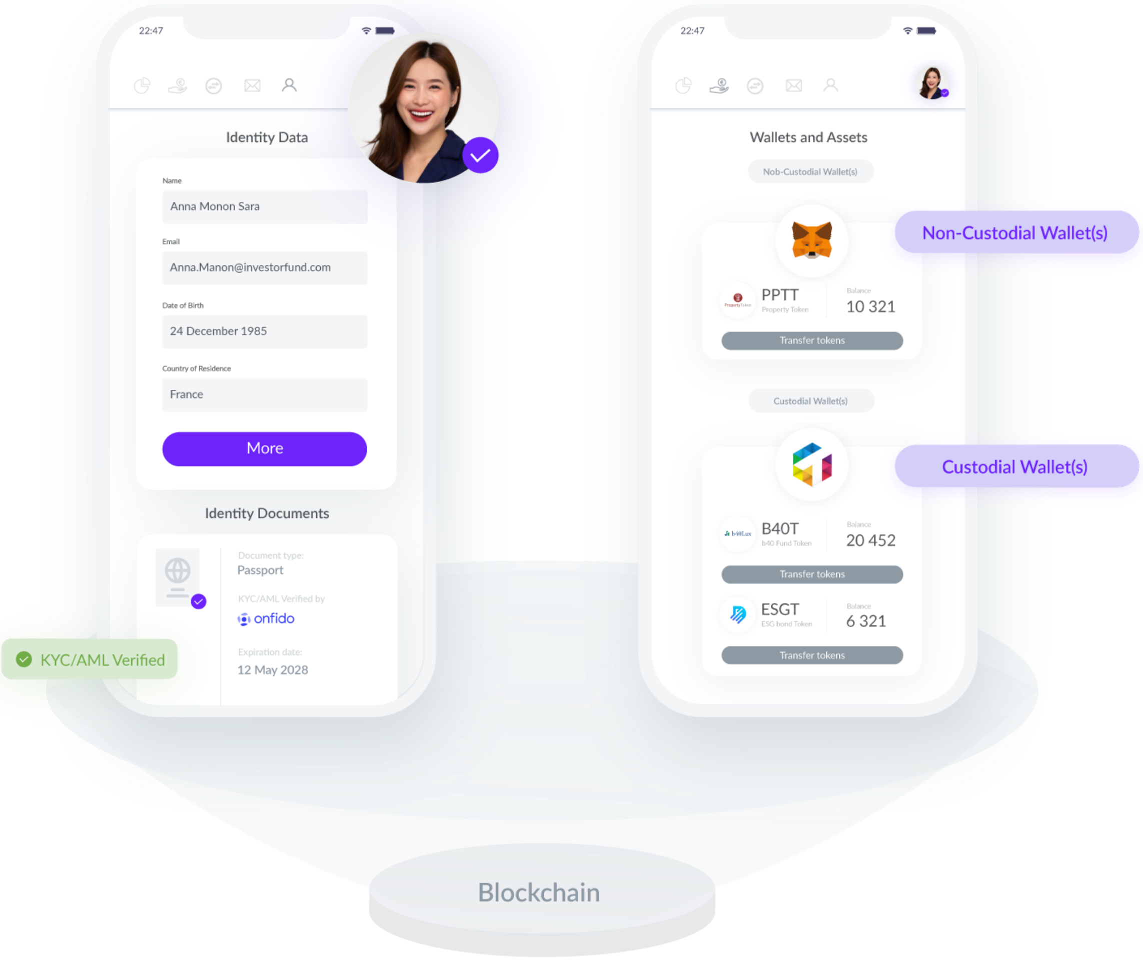
Any blockchain user can easily get its own onchain identity, for free.

ONCHAINIDs can be managed directly on the ONCHAINID web app, but also on other front-ends provided by authorised service providers. For example, the issuer of a security token applying compliance rules with ONCHAINIDs may propose an investor portal to its clients and allow them to directly manage their identities from there. This use case is already live with dozens of security token issuers using Tokeny's solutions[5].

Managing an ONCHAINID as an Identity Owner means managing:

- Identity information
- Wallet(s) authorised to manage the identity
- Claims, meaning the onchain proofs signed by trusted third-parties
- Accesses to the identity information

[5] https://tokeny.com/t-rex-platform/



Name: Anna Monon Sara
Email: Anna.Manon@investorfund.com
Date of Birth: 24 December 1985
Country of Residence: France

Document type: Passport
KYC/AML Verified by: onfido
Expiration date: 12 May 2028

PPTT Property Token, Balance 10 321
B40T b40 Fund Token, Balance 20 452
ESGT ESG bond Token, Balance 6 321

Enrich and control identity information

An ONCHAINID has a unique blockchain identifier: its smart contract address. **In this smart contract, proofs of identity data are signed by Claim issuers**. Several service providers can store information about an Identity, while keeping this information outside the blockchain. By default, Tokeny would primarily act as the core developer of the ONCHAINID system and securely host the basic data of identity owners in an encrypted database. Other service providers and institutions could also issue ONCHAINIDs and store information: Banks, governments, communities and many others could easily become compatible with ONCHAINID. The idea is not to centralise the data hosting, it is to digitise the proofs of data and to centralise these proofs in an identity smart contract under the control of the Identity owner.

For instance, the initial service provider that deployed the identity smart contract on the blockchain could initially store the identity owner's name, email address, postal address, country, website, and maybe other pieces of data about the identity. Another service provider could store a verification of the identity owner on sanction lists, another one could store the passport copy, etc. A service provider that stores and diffuses information about an Identity is called an *Information Provider*.

Any *service provider* would be able to request any relevant information from the *Information Provider*. The Information Provider provides the data only if the *service provider* is allowed by the identity owner to access the information. **The *identity owner* has complete control over what information is shared with which service providers.**

Onchain identity proofs (claims)

Claims are certifications of identity data visible in the ONCHAINID smart contracts. They can be obtained from several sources:

- From the identity owner (so-called "self-attested" claims),
- From trusted claim issuers, or technically anyone the identity owner allowed to add claims to its identity.

They are stored in a ClaimHolder contract (ERC735) owned by an Identity contract (ERC734).

Issued claims can be removed from a ClaimHolder contract by:

- The identity owner (it has the ability to remove ANY claim),
- The issuer of the claim to be removed, or technically anyone the identity owner allowed to manage claims on its identity.

Note that there is NO WAY to verify that the identity smart contract is strictly compliant with the ONCHAINID standard or if it has been modified. It is therefore important for users to generate their ONCHAINID via an official application, and to avoid self-deployments of identity smart contracts.

A claim issuer may only issue one claim per type per Identity contract. It will be stored by a unique identifier composed with the issuer’s blockchain address and the claim type. Issuing a new claim for the same type will override the first instance. A claim issuer has NO CERTAINTY that the claim will be added or updated, as the Identity contract implementation could deny the update. The only security is that NO ONE can fake the claim issuer signing key, thus **a valid claim can only be issued by an approved Trusted claim issuer**.

Claims may be related to sensitive data. **To respect privacy, this data cannot be publicly stored on the blockchain**. A trusted claim issuer should store the data they checked in a secured off-chain database, and refer to this data in the onchain added claim. By default, ONCHAINID core developers already provide the complete data management system.

To ensure compliance, a hash of this data should also be stored with the claim added to the Identity. As external data is not accessible from within the blockchain when transactions occur, the claim should be self-explanatory to validate compliance for the given token, without exposing sensitive data. When the claim is related to data that is part of an exhaustive list of possibilities (i.e. gender, country of residence, age, ...), the hash is not enough to keep the data private as it is pretty easy to find the private data by iterating on a limited list of possibilities, hence, in this case, it is important to hash a concatenation of this data with another data that is not part of an exhaustive list (e.g. last name or first name of the user).

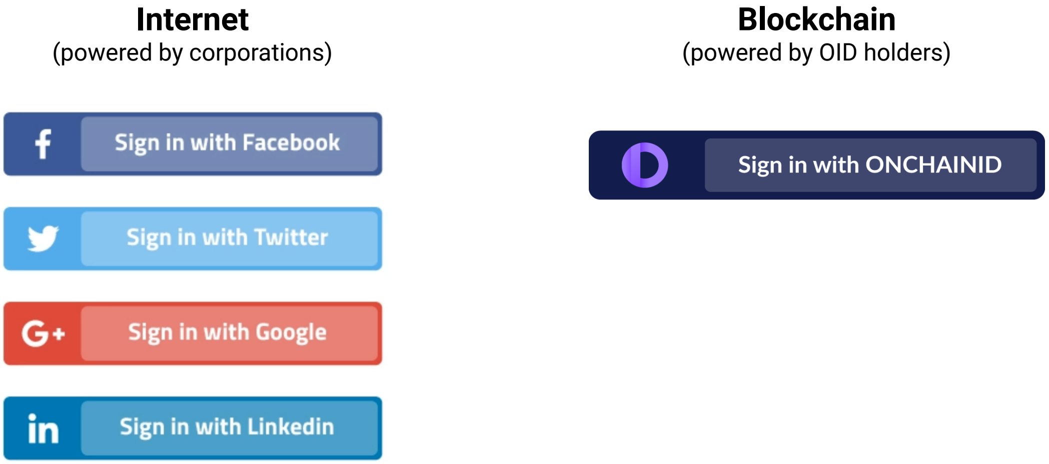
Some claims are therefore shareable between DeFi protocols and between tokens of multiple issuers (for instance: accreditation status) and are called *Generic Claims*, or between token for a same issuer (for instance, the fact that the investor is approved for token investment for a set of tokens) and are called *Specific Claims*. Specific claims can be customised per protocol, per token or per issuer (for instance, the token issuer asks for a claim check that will allow him to know that the investor satisfies a set of criteria like country, occupation, in a list of approved ones that he configured with the claim issuer). Generic claims are public statuses that usually have an expiration date.

To generate a claim, a claim issuer can ask the identity owner all data it requires through a custom User Interface, mail exchanges, research... Some claim issuers allow identity owners to share their information with other claim issuers that implements an OAuth[6] client. The list and content of data shared are explicitly displayed to the user when an access is requested by an application. A claim can be requested by anyone for an onchain identity.

[6] OAuth (Open Authorization) is an open standard for access delegation, commonly used as a way for Internet users to grant websites or applications access to their information on other websites but without giving them the passwords. - Wikipedia

Sign up/Sign in with ONCHAINID

An ONCHAINID allows its owner to login to a website or a protocol without a password by using their Identity as it is possible with Social Providers such as Google, Facebook, Apple, Microsoft, etc.



The compatible website will display a Sign in / Log in or “Connect with ONCHAINID” button. **When a user attempts to login, the server generates a challenge to be signed using a blockchain wallet linked to the relevant onchain identity**. The server can request access to some Information and claims about the identity to speed up the registration process.

The following process explains the authentication flow for the ONCHAINID connect. To summarise, a website requests access to a certain set of information, and allows the connection once it has all the access it requires. The website (or service provider) can request more access, but it requires a new signature from the identity owner for each request.

An identity owner can share, at the request of the service provider, a list of data related to its onchain identity. The identity owner signs this list, and the service has access to this list only. This may include the First and Last Name, Email, Address, or any claim data stored by the identity service provider.

Once the onchain identity is connected, the identity owner will be able to share additional data such as other claim data or information stored by other Information Providers or claim issuers.

There are two ways to grant access to information:

- **Immediate grants**, which only allow access once to information,
- **Persistent grants**, which allow longer-term access until the grant is revoked by the identity owner.

ONCHANID gives the identity owner control of its onchain identity. When an identity owner decides to share information about the onchain identity with a third-party service provider, an explicit signature of an “access challenge” is requested.

This allows Information Consumers (entities needing the data) to request access to identity data such as:

- Basic Information data (first name, last name, email, phone, address).
- Claim data (access to a precise claim content)

By signing an access challenge, the identity owner creates an Access Grant for a service that can be revoked if needed. *Note that a revocation will not delete the data eventually stored by the service provider, but will prevent the service provider from accessing any data that can be subsequently updated.*

When an identity owner revokes an Access Grant, the related service provider is no longer able to access the data.

Resources

Technical documentation: https://docs.tokeny.com/docs/onchain-identities

Use cases

Onchain Assets ownership

As explained previously, the allocation and enrichment of ONCHAINIDs make it possible to identify individuals, companies and assets on the blockchain. As a consequence, it is possible to execute actions (transactions) on the blockchain that take into account the different parameters of these identities. It is therefore also **possible to create "permissioned tokens", controlled by a central issuer, that can only be transferred to eligible ONCHAINIDs, and can be recovered in case of loss of private keys**. This protocol for permissioned tokens already exists, and is called T-REX (Tokens for Regulated Exchanges) and recognized by the Ethereum community as the ERC3643. For a few years it has been used for security tokens as many compliance rules must be applied to financial instruments, but also for any type of assets where an issuer of a token needs to track and guarantee the legal ownership of the token. For example, **a custodian could immobilise shares, paintings, Non-Fungible Tokens ("NFTs"), stablecoins, or bitcoins and represent them with T-REX permissioned tokens**. These tokens can be deployed on any Ethereum Virtual Machine compatible blockchain network such as Ethereum mainnet, Polygon, Binance Smart Chain, etc. Because they are permissioned with ONCHAINIDs, these tokens are recoverable: As long as a token holder can prove its identity to the issuer, it can recover its tokens. Even if the wallet changes on the blockchain, the owner does not change because the lost wallet and the new wallet are both linked to the same onchain identity. Therefore, **it facilitates self-custody, without the risk of self-custody.** More information about this feature can be found here: https://tokeny.com/tokens-recovery/

Today, if you lose access to your bitcoin wallet or your ERC20 wallet, nobody can help you. With ONCHAINIDs and permissioned tokens, as long as you can prove your identity you can recover any tokens linked to such identity.

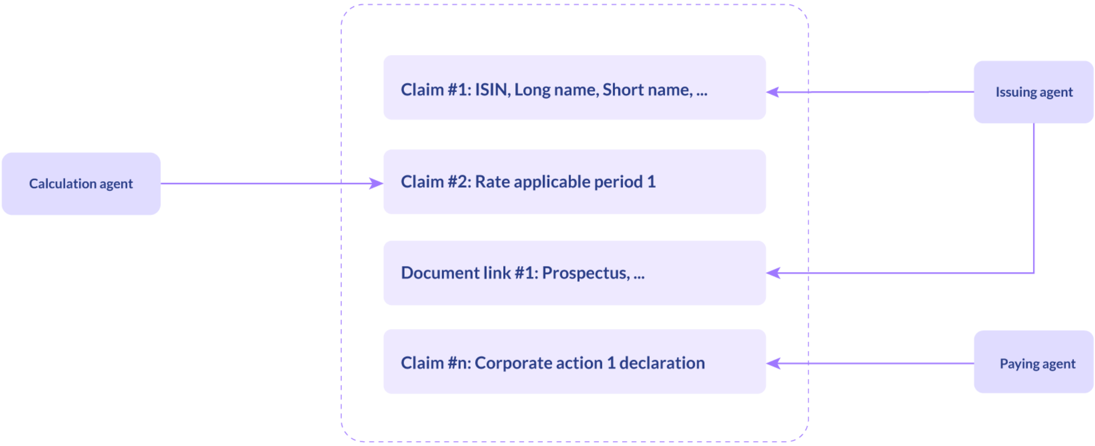
Identities for Assets and Securities

It is already possible to extend this notion of identity to financial instruments and assets by **attaching to the root smart contract of a token or an NFT a container where various data related to the security or asset itself will be stored**. For example, for a security token, some data can be linked and certified onchain:

a) The static data about the financial instrument: name, type (debt, equity, fund, …), date of issuance, maturity date, etc.;
b) The dynamic data of the security will be added by the issuer or its agents throughout the life of the security: dates and rates of cash distributions, corporate actions, shareholder meetings, etc.; and
c) Other "claims" added by trusted parties. This will be particularly useful to receive the

assessments made by the relevant management based on the investment policy of the security, e.g. to make them *shariah compliant* or *ESG compliant* instruments.

Example of ONCHAINID for a financial instrument


Claim #1: ISIN, Long name, Short name, ...
Issuing agent
Calculation agent
Claim #2: Rate applicable period 1
Document link #1: Prospectus, ...
Claim #n: Corporate action 1 declaration
Paying agent

The use of such “security identity” will solve the recurrent issue to access reliable (so-called “golden copy”) and up-to-date information regarding a security. It is to be noted that such “security identities” could naturally be issued for securities issued as tokens on the blockchain but also very well for securities issued in a more traditional manner.

Of course, **many use cases are possible following the same logic**. For example, a real estate developer could deploy an ONCHAINID for a building where the architect, the electric company and others would provide and certify information. It would help owners, potential buyers and other entities to evaluate the building depending on their expert certifications (economic value, energetic impact, etc.).

DeFi for institutions

DeFi is growing but still under development. Regulation is struggling to keep up with the high rate of change, but the obligations of institutions are no less important. As we have seen with the launch of AAVE Pro (rebranded in AAVE Arc), **there is a demand from institutions to invest heavily in DeFi, but in a framework where all the counterparts are known and / or controlled, at least in terms of KYC.** The ONCHAINID protocol allows the various counterparties to prove their eligibility and verify that of the others, without revealing the identities of all the participants.

Thus, for example, the identity of the deployer of DeFi protocol smart contracts can be verified to ensure that it does not appear on the main sanction lists. Also, it is possible to restrict the use of the protocol according to certain criteria, or to block / unblock functionalities according to attributes linked to the identities. We can easily imagine restrictions by type of investor (individuals vs corporates), by country, etc.

Universal login & digital identity

First and foremost, ONCHAINID facilitates compliance by helping its users to prove that they are “compliant” to websites, DeFi protocols and token issuers. This is possible thanks to the “blockchain account” held by the owner of the identity. Since this identity is digital, it was made in such a way that it can be linked to an email, and to one or more wallets. It is also compatible with most types of authentication keys.

Crypto-asset marketplaces can therefore use the **ONCHAINID login to facilitate the onboarding of their users, request access to the identity proofs** they need, and easily apply the compliance rules to their users, without taking possession of their assets.

IOT & Oracles

We interact with computer programs contained in everyday objects at a continually increasing rate. Think of your smartphone and your car for example. Also, these programs interact with each other and become interoperable. Soon, thanks to the blockchain, such programs will not only share information but also value. **Providing ONCHAINIDs to objects will help to identify each of them onchain and to manage their roles and permissions.**

As an example, you could park your car in a Parisian street, and the car would automatically be detected by the sensor of a meter that will request information to the car in order to know its owner and charge its account with the parking fees. If the car has an ONCHAINID, its owner account would be a Claim (proof), certified by the national car registry. The meter could also verify at the same time that the car got the Crit’air ecologic pass[7] by checking this other claim.

[7] The French Crit'air air quality certificate is a vignette issued to show a vehicle's compliance with European emission standards.

The OID token

Decentralising ONCHAINID

If today your Google account is your main authentication and identity system on the Internet, it is largely thanks to the critical mass of users using this same system. Many sites and applications have an interest in facilitating the connection with Google to simplify the creation of accounts for their users. **The more users there are, the more a virtuous circle is created and promotes the development of an ecosystem of compatible services**.

> It is essential for an identity system to reach a reasonable critical mass of users and partners to create positive network effects for its users.

In order to reach this critical mass as quickly as possible, Tokeny, the company that initiated the ONCHAINID system, has decided to open up the governance of the protocol by issuing a utility token, the “OID token”, to incentivise the various players in the value chain. Unlike the Internet of Information controlled by powerful corporations, blockchain enthusiasts want the Internet of Value to be controlled by its users. **It is therefore mandatory to decentralise the main identity protocol**.

Issuing a native utility token at the heart of the system is the fastest way to this decentralisation: the OID token is the utility token used in the ONCHAINID ecosystem. The holders of OID tokens are inherent to the development of the ONCHAINID ecosystem. The OID token is compatible with the ERC20 standard.

OID tokens effectively allow their holders to participate in the governance of ONCHAINID and **interact more broadly with the protocol, its applications, and its participants.** The token will incentivise users, partners and developers that are part of the ecosystem. It may also enable additional functionalities to be unlocked in the future. Holders of the utility token can be consulted on proposals that affect the direction of the ONCHAINID project, including decisions concerning:

- the token supply and distribution mechanisms to incentivise stakeholders;
- new features and improvements of the protocol and its applications; and
- potential monetisation schemes for ONCHAINID identity owners and OID token holders

The OID tokens are utility tokens and as such they are not intended to be or qualify as financial instruments, securities, or security tokens under the laws of any jurisdiction. However, it is possible that the OID tokens may qualify as a financial instrument, security, or security token in your jurisdiction, or that the acquisition of the OID tokens is a regulated or prohibited activity, and in neither of these cases the issuer may be liable for the same or assume any responsibility in connection therewith.

Governance

The governance of the ONCHAINID ecosystem will be managed by both core developers (who would be providing propositions), and token holders (who would be consulted on and vote on such propositions). OID tokens will give token holders the right to be consulted on propositions, but such consultation right is non-binding and as such the result of the consultation is not binding on the issuer of the OID tokens, who may unilaterally decide to adopt another proposition than the one voted for by the majority of the token holders. The voting power of token holders would be related to the size of their holdings at a fixed blockchain block on which the voting will close.

In order to participate in the governance consultation process, each token holder must also own an ONCHAINID smart contract. The consultation process will take into account the holdings of each wallet linked to the ONCHAINID of the token holder, this way it is not necessary for a token holder to vote with each wallet it owns in order to participate in the governance consultation process (in case a token holder owns several wallets).
The voting power per token will be equivalent to 1 OID token = 1 vote.

Voting propositions may take 4 forms:

- **A simple proposition** is submitted to the community with a boolean answer requested (yes or no), in this case the answer collecting more than 50%+1 of the votes will be taken into account by the issuer.
- **A multiple choice proposition** is submitted to the community,
    - with a single answer requested, in this case the answer collecting the most votes of the votes will be taken into account by the issuer, or
    - with the possibility for voters to choose several propositions that satisfy them, in this case the answer collecting the most votes of the votes will be taken into account by the issuer, or
    - with the possibility for voters to choose several propositions that satisfy them and to add a preference order on which they consider the various propositions, the vote count will then use this order to ponderate the voting power on each proposition and in fine the answer collecting the majority of the ponderated votes will be taken into account by the issuer.

Token Generation Event:

Token issuance

Tokens will be issued at the end of the token sale.

OID tokenomics

Overview
Token supply: 1,000,000,000 OID tokens

Groups	OID tokens
Community	300,000,000
Liquidity	200,000,000
Developers	300,000,000
Partners	200,000,000

During the private sale, detailed information is available on request.

Details
Token Allocation

Developers: 300,000,000 OID

- Tokeny: attribution of 190,000,000 OID for the past 3 years of development
- Intech: attribution of 10,000,000 OID for their contributions
- Treasury for future developments: 100,000,000 OID

Partners: 200,000,000 OID

- Marketing & distributors
- Strategic Financial Institutions
- Claim issuers adding identity proofs onchain

Community: 300,000,000 OID via token sale

- Seed Round
- Strategic Round
- Private Round
- Public Round

Supply Reduction
If all tokens are sold during the token sale, then 300M tokens are sold and $8M are collected, which allows the issuer to initiate the DEX Liquidity at a price of $0.04 for 200M tokens.

In case the total supply of the private rounds is not sold, these tokens will then be available for the public sale. In case all 300M tokens of the private and public sales are not sold at 100%, the remaining tokens will be burned and the DEX liquidity will be initiated at the price of $0.04 per token with the amount of money collected, the remaining available tokens for the liquidity will be burned as well.

Supply Releasing Schedule

Developers

- **Tokeny Solutions** tokens are vested with 15% of the tokens unlocked every quarter;
- **Intech**'s tokens are vested with 15% of the tokens unlocked every quarter;
- **Treasury for future developments** tokens are locked for one quarter and then vested with 10% of the tokens unlocked every quarter tokens. Maximum amount of unlocked tokens per quarter is 10%, no matter if all the tokens were taken the previous quarter or not, which means that the vesting could last for more than 10 quarters, depending on the participation of the community and rewards unlocked every quarter.

Partners

Tokens for partners are locked for one quarter and then 5% are unlocked each quarter. Maximum amount of unlocked tokens per quarter is 5%, which means that the vesting period could last for more than 20 quarters depending on the participation of the community and rewards allocation.

Liquidity

Tokens added to the liquidity pool on Quickswap, “LP tokens" are locked for 1 year, no liquidity can be withdrawn the first year. Then 6.24% of LP tokens will be unlocked each quarter.

Community

- **Seed Round** tokens are locked until 3 months after DEX listing and then 10% are unlocked each quarter;
- **Strategic Round** tokens are locked until 3 months after DEX listing and then 15% are unlocked each quarter;
- **Private Round** tokens are locked until 3 months after DEX listing and then 20% are unlocked each quarter;
- **Public Round**, 50% of the tokens are locked for one quarter after DEX listing and then 10% are unlocked each quarter.

Roadmap

2018

✓ Smart contracts

Smart contracts and software protocols for individuals and businesses/institutions was created: this is primarily to support the use case of issuing security tokens under the T-REX permissioned tokens protocol

2019

✓ API & SDK

The Identity API allows you to create, update and request identities on the Tokeny ecosystem, and run some requests on the blockchain such as claim emission and retrieval, ONCHAINID updates and more.

2020

✓ T&Cs and Compliance

Comply with data protection regulations (e.g. GDPR)

✓ ONCHAINID Automated Generation

ONCHAINID automated generation and deployment for security tokens investors

2021

✓ White-labeled UI

ONCHAINID management UI on white-label investor portals for security tokens

✓ Built-in Wallet

On-demand provision of an integrated regulated custodial wallet

S1 2022

○ Webapp Version 1

- ○ Qualification of users and ONCHAINID generation
- ○ Identity data and documents management
- ○ Listing of the associated wallets
- ○ Listing of the identity claims (onchain proofs)
- ○ Viewing, granting and revoking access to their data to 3d parties

○ Universal Login

○ OID Token Issuance Coming Soon

○ OID Token Listing

S2 2022

○ Webapp Version 2

- ○ On demand built-in custodial and regulated wallet
- ○ Improved associated wallets management
- ○ Multi-assets portfolio view
- ○ Username(s) and ENS management

○ ONCHAINID Identification

Additions by the ONCHAINID system itself of a generic claim confirming the identification of the Identity Owner

○ ONCHAINID KYC

Addition by the ONCHAINID system itself of a generic KYC proof confirming the "regulatory acceptability" of the Identity Owner

2023

○ ONCHAINID Chromium Extension

Wallet aggregator in a Chrome extension allowing to directly sign transactions

○ Compatibility with eIDAS

Connect national european IDs to ONCHAINID smart contracts (eIDAS proof-of-concept already realized)

○ ONCHAINID Signature

Depending on eIDAS compatibility

○ ONCHAINIDs for Securities

○ ONCHAINIDs for Assets

○ Data storage on IPFS for claim issuers

Ecosystem: Team and Partners

A growing ecosystem

For nearly 4 years, the teams developing ONCHAINID have evangelised the market by explaining the T-REX protocol for permissioned tokens, which notably allows financial institutions to tokenise securities in a compliant way, on public blockchains such as Ethereum or Polygon. Tokeny is **already in contact with many institutions and service providers**, such as asset managers, fund servicers, banks, auditors, government entities and KYC solutions.

Much of these business relationships are already using ONCHAINID for their investors or to certify information on the blockchain. Most of them will therefore be delighted to be able to join the ecosystem's decentralisation initiative through the issuance of the OID token. Thanks to the publication of this whitepaper, more concrete discussions are underway, and partnerships may be announced one after the other.

Different types of stakeholders can add value to the ONCHAINID ecosystem. Partners are mainly actors who usually exercise a role of trust. Thanks to identity certifications, they will be able to help digitise this trust and benefit the blockchain ecosystem. Developers are building and maintaining the system on a daily basis, and the growing community will play key roles in the success of ONCHAINID.

Developers

Developers are essential to the proper functioning of the ecosystem since they create, maintain and develop the smart contracts, APIs and web interfaces necessary for the use of ONCHAINID.

Several companies and groups of individuals are already involved in the technical developments of ONCHAINID:

- ***Tokeny Sàrl -*** *Tokeny.com*

Tokeny allows financial actors operating in private markets to compliantly issue, transfer and manage securities using distributed ledger technology, enabling them to improve asset liquidity. The Luxembourg-based company is the leader in securities tokenisation and in 2020 was named one of the top 50 companies in the blockchain space by CB Insights. They are backed by Euronext NV, the pan-european stock exchange group.

Since 2018, Tokeny is developing ONCHAINID (protocol and softwares) as the needed compliance component of the T-REX protocol for security tokens. Most of the developments were financed thanks to a fundraising of 5 millions euros entirely subscribed by Euronext in July

2019. Tokeny is also a member of the ERC725 Alliance. After the OID token issuance, Tokeny will continue to act as the core developer of the ONCHAINID ecosystem.

- ***InTech -*** *InTech.lu*

InTech is a Technology and Information Systems Consulting company founded in 1995 and becoming a subsidiary of the POST Luxembourg group in 2015 (government owned). The company employs more than 120 collaborators specialised in the design and the realisation of specific IT solutions built from reusable software components. Combining the synergy between knowledge of a business and mastery of technology, InTech supports its clients in their digital transformation and the evolution of their information system.

For several years, InTech has been offering its blockchain expertise to financial and government players in and around Luxembourg. Many projects have already emerged and are in development, such as EDDITS, aimed at connecting blockchain identities with the European standard eIDAS via LuxTrust. InTech is also heavily involved in government blockchain projects and projects relating to the investment fund industry. They also joined the ERC725 Alliance in 2018.

- ***Individual developers and software companies***

As the ONCHAINID protocol is open source, **individual developers or IT development companies are invited to contribute**. If their contributions are accepted and taken into account in the protocol evolution, OID tokens will be distributed in order to reward them.

- ***Polygon -*** *Polygon.technology*

Polygon is a protocol and a framework for building and connecting Ethereum-compatible blockchain networks. They aggregate scalable solutions on Ethereum supporting a multi-chain Ethereum ecosystem.

Polygon already allows many issuers of DeFi tokens and protocols to express their full potential thanks to an impressive speed of blockchain transactions and insignificant gas fees. Since spring 2021, ONCHAINIDs have mainly been deployed on Polygon and the possibilities offered by **the advantages of this network have increased the use cases of identity and compliance exponentially**.

Polygon teams are looking for serious projects to accelerate the adoption and ensure the sustainability of DeFi. We believe that ONCHAINID responds concretely to these challenges and will therefore seek help from Polygon in order to democratise the use of ONCHAINID.

Partners

Partners bring value into the ecosystem by bringing their credibility and resources. They mainly help **to ensure trust and compliance in the ecosystem,** but also participate in the **distribution of ONCHAINIDs** by bringing their customers, audience and networks.

- ***Government entities***

Governments are the primary issuers of identities. The vast majority of them **have started a process of digitising these national identities** in order to make life easier for their citizens and improve their management. By issuing identity standards (eIDAS, NDI, etc.) they can facilitate the identification of participants.

More broadly, their validation of the ONCHAINID model (use on their applications, licenses, authorisations, etc.) for the application of compliance rules on the blockchain will help accelerate adoption.

- ***Big 4, Auditors and Consulting firms***

Auditors play an essential role in finance by ensuring the veracity of information and carrying out studies of all kinds. **The results of their work can benefit the ecosystem if they add evidence to the blockchain and act as a trusted actor.** For example, a big 4 can enrich the ONCHAINIDs of investors by acting as KYC agent of an issuer of tokenised securities, or sign the verification of the annual accounts in the identity of a company, or even audit the smart contracts of a protocol and add the onchain proof to the ONCHAINID of the protocol.

- ***Custodians and digital assets custody solutions***

Custodians and digital asset custody solutions can play an important role for Permissioned Tokens and for Permissioned DeFi. Indeed, they **provide solutions to immobilise assets and to represent them on the blockchain** (tokenisation) on a permitted model, which guarantees immutable ownership with the ONCHAINID system.

Also, the best way to whitelist wallets is to link them to ONCHAINIDs. This makes it possible to create a collaborative and re-usable whitelisting where everyone can enrich and consult proof of identity.

- ***KYC solutions***

Many KYC / AML / KYT solutions exist. They speed up user verification and automate part of the user onboarding process. However, they very rarely take responsibility for verifications, so it is always the exchanges, issuers of tokens and DeFi protocols that bear the responsibility. Some allow you to re-use your information more easily and try to create mutualised KYC solutions.

All these solutions are a priori compatible with ONCHAINID. Indeed, the system allows KYC agents to add the verification proofs made by KYC solutions on the blockchain. It is then up to other parties to trust this evidence or not.

- ***DeFi protocols***

In order to attract institutional users, DeFi protocols (lending, AMM, DEX, etc.) will have to adapt to their regulatory obligations. This does not mean centralising or re-intermediating the service, but finding a way to **control the eligibility of participants in the protocol according to regulatory criteria.**

This *Permissioned DeFi* trend is starting to emerge. For the moment, protocols are duplicated and closed to institutions with a unique third party who validates the participants. A whitelisting of ONCHAINIDs would allow more flexibility and perform these identity checks directly on the blockchain, while ensuring better management of confidential data.

- ***Distributors and referencing partners***

Many partners can help with **listing and distributing OID**. The more OID will be visible on platforms, exchanges, dapps, wallets and marketplaces, the more the number of users of the system will increase.

- ***Financial institutions***

Financial institutions such as banks, stock exchanges, asset managers, fund servicers and broker dealers play a role of trust in traditional finance. They are used to acting as service providers for securities issuers and investors. The value chain is currently too fragmented because the technical infrastructure is not shared. With public blockchains and ONCHAINID, these **service providers will be able to digitise the trust they bring into the ecosystem, without re-intermediating the entire chain**. They will act as a trusted agent to allow more security, without however intervening as holders of the assets in place of their owners.

Community

- ***Users***

Obviously, **the most important thing for the development of ONCHAINID is that the community of users interacting with the protocol grows larger every day**. Anyone can theoretically become an ONCHAINID user. The more users there are, the more key partners will be interested to offer their services on this same standard. It will therefore become increasingly simple, quick and useful to use your ONCHAINID when interacting with a DeFi protocol or with permissioned tokens.

- ***Liquidity providers***

In order to guarantee the ease of use of the system, its compatibility with Dapps, and that everyone can participate in the governance of ONCHAINID, it is **essential to have a share of the OID tokens made available on DEX and AMMs** such as Uniswap, Sushiswap and Quickswap. OID holders who make them available in the liquidity pools will be rewarded according to the protocol concerned. These market makers play an essential role in the ecosystem.

Join the ONCHAINID community

Telegram community: https://t.me/onchainid_chat
Telegram official news: https://t.me/ONCHAINID