Self-sovereign identities in the crypto industry

HOW SELF-SOVEREIGN BIOMETRICS HELP CRYPTO COMPANIES TO ADDRESS INDUSTRY CHALLENGES

YoonIK

Table of Contents

Introduction

Cryptocurrencies were designed to provide people with a way to engage in financial transactions without having to depend on banks or financial institutions. But with greater adoption comes greater responsibility. Despite the “crypto winter” predictions, global adoption of cryptocurrency has surpassed expectations this year.

Crypto assets are also getting more attention from regulators around the globe, trying to prevent fraud and money laundering in the crypto industry. To have a big impact on the financial industry, cryptocurrencies need to be trusted. So, there is a pressing need for crypto companies to be able to verify the ID of their customers, with some countries already requiring crypto firms to comply with KYC/AML procedures to operate.

The road to compliance can be tough and some exchanges may be reluctant to implement KYC procedures for fear it will negatively affect their customers’ experience. Meanwhile, data breaches keep making consumers wary of giving personal information.

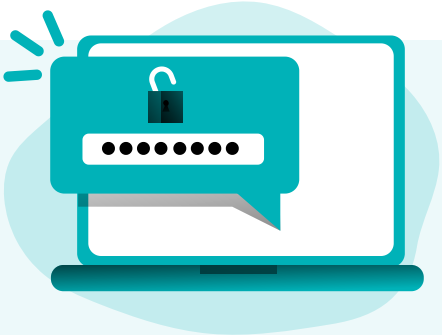
Self-sovereign identity (SSI) presents an opportunity for crypto companies to offer users a decentralized way to manage their identities while complying with legal requirements, without depending on third-party providers to store and manage users’ data.

1. A brief overview of self-sovereign identity and biometrics

There is a growing concern among businesses and individuals about the security and privacy of credentials. Millions of dollars have been spent on security and privacy since the early days of the internet. In spite of this, hackers can still find a way around vulnerabilities to cause damage. **Every day, personal information of millions of users is exposed as a result of data theft from companies** with severe consequences, including damage to the brand's reputation as well as hefty penalties and fines.

Most crypto exchanges and wallets use centralized and federated identity management systems that make them **vulnerable to large-scale hacks and data breaches**. Over time, password complexity has increased to improve resilience and security against cybercriminals and hackers who automate the combination of characters to crack passwords. In general, the longer and more complex the password, the better, since decryption times increase exponentially. However, users tend to reuse passwords multiple times or pick obvious passwords, making it really easy to hack their credentials.

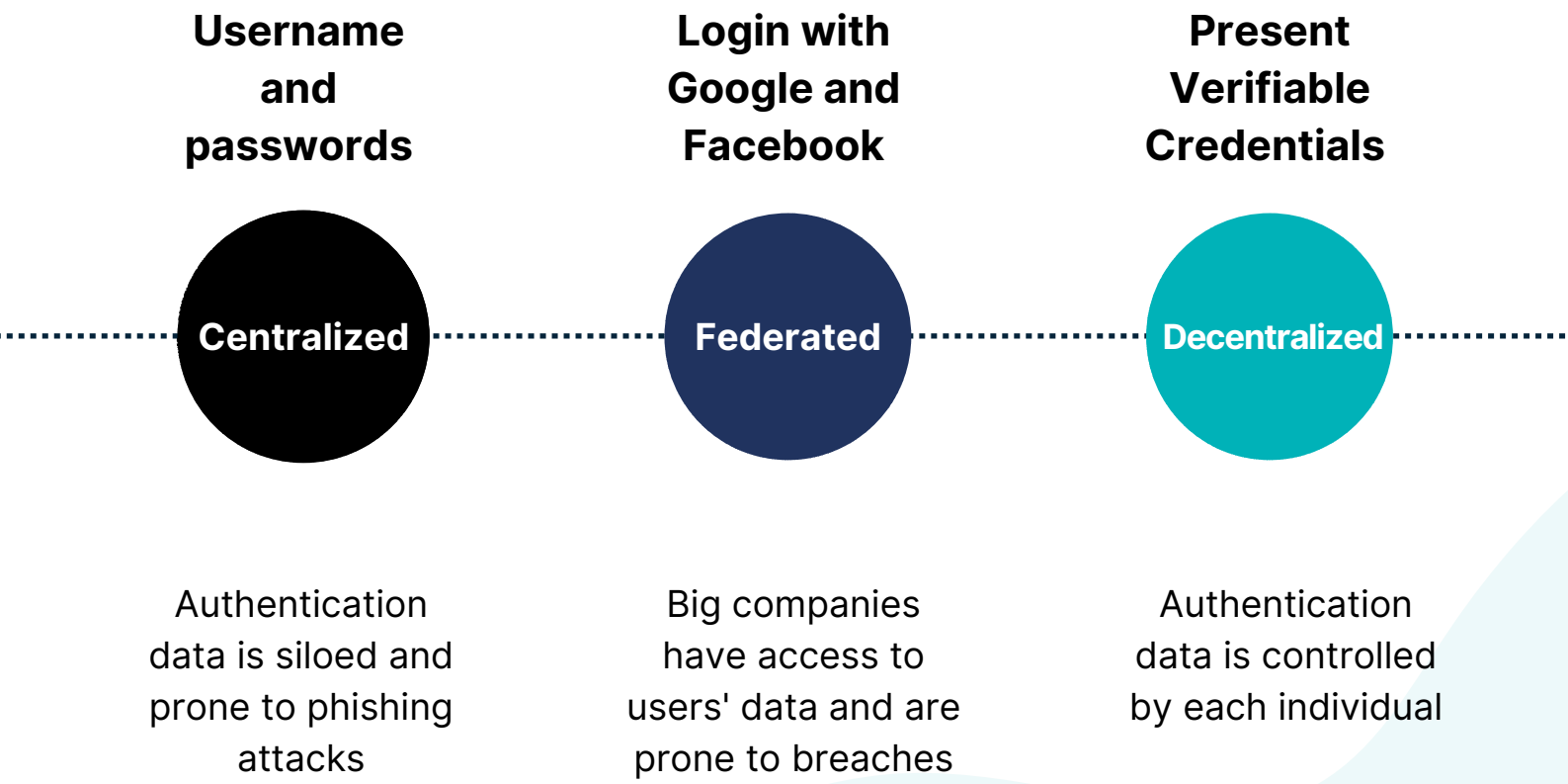
On the other hand, using federated identity systems (e.g. signing in with a Google or Facebook account), credential system providers can store and track people's online activity without their knowledge. As the Cambridge Analytica scandal showed us, **being held by a large company doesn't mean our data is safe**.



81 %

of company data breaches were caused by misuse of passwords.

The increase in data scandals, the growing concern about privacy, and the advancement of technology led to the push for the decentralization of identity. A self-sovereign identity model gives individuals **full control** over their digital identities without involving third parties to store and manage data. Digital identities, in this context, refer to data that is online and can be traced back to an individual or organization, including usernames and passwords.



SSI relies on so called **zero-knowledge proofs** where credential holders' privacy is protected. With verifiable credentials, users do not have to disclose their actual details in order to prove their identity.

Self-sovereign biometrics marries the concepts of decentralization with biometrics in a privacy-first solution capable of putting users in control of their data and their privacy.

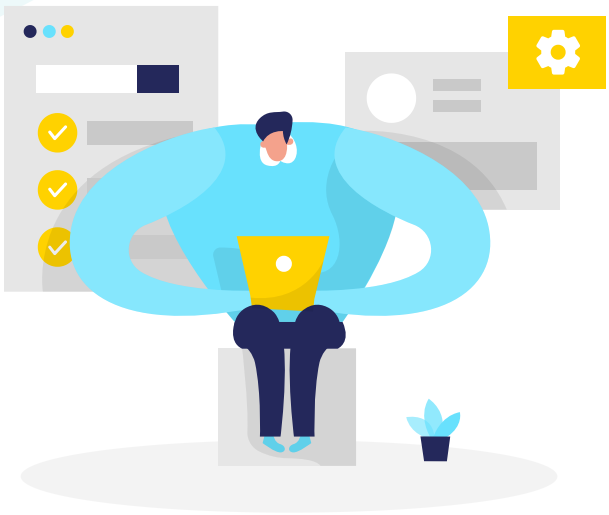
2. Addressing crypto industry challenges with self-sovereign biometrics

Most crypto companies are not satisfied with the existing KYC and identity approaches. SSI can provide them with an identity layer that creates a bridge between an **ownership-based identity approach** and **legal and security requirements** that will ultimately be the key to cryptocurrency's wider adoption. Furthermore, a self-sovereign identity approach in the crypto industry promotes **trust and speed**, reinforces **privacy and security** and offers **more flexibility and agility** for both users and the crypto company.

The compliance challenge

Let's start with the basics. The legal status of crypto companies depends on the country where they're based and the countries where they operate. However, generally speaking, **almost every country now requires exchanges to comply with AML/KYC procedures**. AML stands for Anti-Money Laundering and it's a set of measures that countries define as mandatory to prevent financial crime. KYC stands for Know Your Customer, and it falls under AML measures.

KYC is a set of steps a business must take to verify customers' identity. This includes information such as legal name, date of birth, address, and proof of identity through an ID card. In the past few years, KYC checks have become mandatory for many more crypto asset transactions in several different jurisdictions.



By introducing KYC requirements in cryptocurrency custodial wallets and exchanges, regulators are trying to **reduce fraud and risk factors** to **give customers a high level of trust** when participating in any kind of crypto assets transaction.

During the KYC process, **crypto companies will need to verify and collect customer's personal data**, which includes legal name, date of birth, legal address, and proof of identity (through an ID card, or others).

KYC procedures come at a cost. Crypto exchanges face many challenges regarding traditional KYC compliance, including high costs, security issues, and ever-changing regulatory requirements. The approach varies from company to company. While many exchanges companies will opt for building their own compliance teams, others will outsource this KYC procedure to third parties by sending documents for verification. Either way, it comes with a high cost. Furthermore, manual verification can take a few hours or even days, causing a huge drop-off rate at onboarding.

The KYC regulations for cryptos are expected to evolve rapidly over the next few years. There will be more frequent and in-depth crypto KYC procedures as the level of regulation increases. Furthermore, KYC requirements vary by country, so exchanges operating in several geographies may have to deal with multiple KYC requirements. **As regulation grows in number and complexity, exchanges will need to scale KYC crypto procedures**. Traditional, manual KYC procedures won't cut it anymore.

Third-party KYC: a problem of security

In 2019, the major crypto exchange Binance was victim of a security breach that exposed sensitive KYC data. Apparently Binance's KYC data was handled by a third party, leading to a debate about whether exchanges should - or shouldn't - handle KYC data in-house to avoid data leaks.

Despite all the challenges that come with KYC compliance, exchanges can take benefits from regulatory compliance, including improved customer transparency and trust and reduced potential for fraud or scams. As the crypto industry evolves, self-sovereign identity can simplify KYC processes, letting users pick which information they want to share, rather than all their ID info. In addition, it offers a reusable KYC process that increases efficiency and security for crypto exchanges and wallets.

The privacy challenge

The second challenge to which SSI can provide an answer is data privacy: a theme more relevant than ever. Since the advent of GDPR at European level (in May 2018), more than 60 jurisdictions around the world have enhanced or presented new privacy and data protection laws. Gartner estimates that, next year, 65% of the world's population will have its personal information covered by privacy regulations. Passwords are not secure, but neither are single sign-on options. Increasingly common in applications and websites, the ability to log in with a Google, Facebook, or LinkedIn account is a major threat to users' privacy as it is often used as a method for logging in. Whenever a user logs in through an identity provider, the provider gains access to the user's personal information. The privacy of millions of users is at stake with such inferential practices.

Along with the need for trust and data protection, there's the issue of "unwanted identity correlation". Through centralized authentication methods, hackers can combine users' identity information that is spread across different platforms but has a common identifier (usually the same email address used as a single sign on option).

Self-sovereign identity keeps the user's information private: it's up to them to decide when, and how, verifiers will access their personal data to grant access to specific products or services.

Stolen single sign-on credentials

Research from BitSight found that more than

25% of the entire S&P 500

have had stolen credentials appear online.

The security challenge

There isn't a universally accepted digital identity that individuals can use across different applications. Each website, each login will ask us for a username and a password or an email address. This poses a problem: **multiple credentials expose the user to a variety of security issues**. Identity theft is a major concern for crypto consumers as, in most cases, the user has no idea their identity has been stolen until it is actively used by the fraudster.

The SSI anonymous authentication method eliminates the need for passwords, codes, or public keys by using users' unique attributes (as the face) to grant them access. Instead of coming up with different usernames and passwords to log in into digital workspaces, online banking applications, and more, users can use their face to have access across multiple platforms.

By eliminating common attack vectors such as passwords, OTPs, email links and SMS as second-factor authentication methods, customers are less susceptible to hackers exploiting gaps in authentication processes.

Crypto cybercrimes (including fraud) totaled
$1.9 billion in 2020
Source: CipherTrace

3. Get started with self-sovereign biometrics

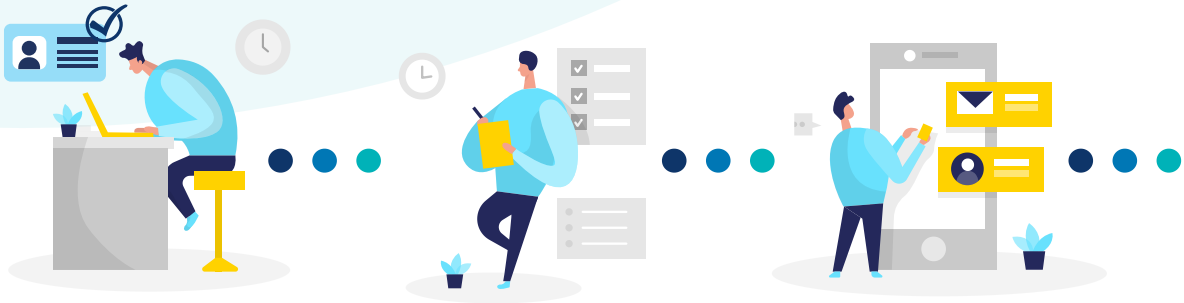
If you want to get started with self-sovereign biometrics in your crypto company, you need to think about it from two different perspectives:

- **What will self-sovereign biometrics do for your company and your users?**
- **What are the underlying technologies and how to integrate them into your application?**

Let's dive deep into each perspective.

What will self-sovereign biometrics do for your company and your users?

First, we'll look at some examples to help you unlock the self-sovereign biometrics opportunities for your crypto company. Below, you can find face authentication use cases that can be applied to several different contexts:



Identity verification

Does the person present own the identity presented?

Onboarding

What data do I need to know in future interactions?

Authentication

How do I know this is my customer at every interaction?

Continuous Authentication

How do I grant this customer interaction hasn't been hacked?

Using face authentication in a decentralized approach, you can **verify your customers identity from the first interaction without the burden of storing biometric templates, personal data or any other private information**. As in the example given, you'll use face authentication not only to ensure your customer John is really who he says he is, but also streamlining the enrollment process and ensuring next interactions are done safely and privately. So, next time John authenticates, you can be sure that it is really him who's buying and selling crypto assets.

Self-sovereign biometrics offer an easy and worry-free way to manage access to crypto wallets and exchanges while **keeping the experience as easy and private as the user expects It to be**.

SSI benefits for users

- Effortless user experience
- Full control over data
- Enhanced privacy

SSI benefits for crypto companies

- Increased conversion/retention rates
- Decreased data breach risk
- Seamless compliance

What are the underlying technologies and how to integrate them into crypto exchanges and wallets?

At YooniK, we are creating awesome tools that any developer can use to improve user authentication and simplify people's lives, by focusing primarily on **privacy and safety**. We know that integrating biometric authentication into your user-facing application can be a daunting and highly complicated task.

Imagine dealing with the problems related to camera integration, analyzing the data stream to check for inconsistency and security vulnerabilities, and integrating a very complex low-level biometric SDK. They have multiple parameters to tune to get an optimized performance. Sounds too complicated, right? That’s why we’ve built our edge software.

As a **developer-first** company, we are always looking into ways to make the integration of secure and private face authentication as smooth as possible. From our experience, the integration of biometric products can be complicated, to say the least. Whether you want to upgrade an existing solution or integrate face authentication systems, you will typically face some problems:

- Complex concepts and definitions not explained in an easy-to-follow manner.
- No human-friendly testbed where to start with a few clicks and zero software integration.
- Super complex low-level SDK with millions of parameters to tune.

Our Face API allows you to perform any face processing (detection, analysis, template extraction) as well as performing verification (image to image matching) or identification (1 to many matching). All requests and responses are encoded in JSON and use a secure HTTPS channel.

YooniK's Face API was **designed to bring face authentication to any application in a developer friendly fashion** by exposing complex biometric functionalities via a simple REST API that can be integrated virtually in any programming language and any environment.

YooniK's Face API use cases

Face detection and analysis

Detect and count the number of faces. In addition, we provide a set of metrics describing each face, such as pose and liveness.

Face images verification

When you need to validate if two face images belong to the same person you can use this functionality.

Face biometric template creation

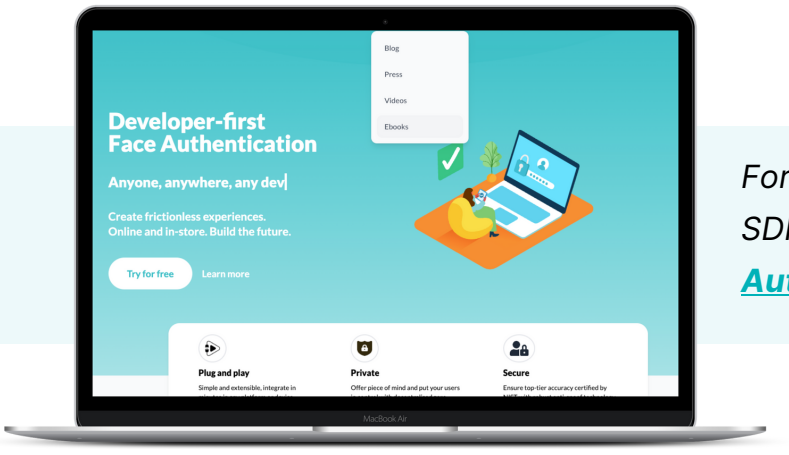
In case you want to create a user base using their face, but you don't want to use images to comply with privacy-by-design at its best, you can convert the face of your user to an irreversible encrypted abstraction of the face image that you can reuse for authentication scenarios.

Face identification

We also enable the use of our state-of-the-art algorithms in identification scenarios (1 against many matching). This process is managed by gallery management API.

Test our Face API for free

You just need to **register** and **subscribe a free plan**. We're integrated with Auth0, Okta and are continuously expanding this list. Feel free to get help on our **discord channel** or get in touch directly with our **support team**.



*For more information about our integration SDKs, check our **github space** and the **Auth0** and **Okta** quick-start guides*

About YooniK

YooniK wants to make identity verification easy for everyone — the user and verifier. That means no more passwords or clumsy codes, and no more waiting to have customers identified, verified, and ready to invest in your platforms.

Furthermore, we find SSI the best way to comply with KYC and other identity-related requirements without storing the customers' data and making your company vulnerable to malicious attacks.

YooniK's products simplify all customer interactions with private, convenient, and secure face authentication on any device. Ranking Top 5 for accuracy in live face matching in the combined business regions of Europe and U.S. in early 2022, as independently certified by the international benchmark, YooniK enables a fully handsfree experience, bringing unprecedented levels of convenience and accuracy when adopting face authentication in daily routines.

Do you need help setting up face recognition in your application?

Send us a message or feel free to book a meeting with our team of specialists, who will be happy to help.

Anything with a look, handsfree and private.

Follow us