

HashbonPass



ANONYMOUS

**NFT
PASSPORT**

**K
Y
C**

ALEXANDER GANIN

GRIGORY BIBAEV

OXXY SHERR

Special Thanks



To our dear people who have invested time and effort into the development of this whitepaper, without whom nothing would have happened!

Sergey Lobanov
Maria Varnacheva
Yuri Golosovker

We really appreciate your contribution to this project.

Contents

SPECIAL THANKS	2
CONTENTS	3
INTRODUCTION	4
ABSTRACT	5
PROBLEM	6
The problem of KYC in DeFi	6
Spam protection and anonymous 18+ checks	7
Applications in the centralized sector	8
Anonymous KYC	9
SOLUTION: NFT PASSPORT	12
Public data of Hashbon Pass	13
Actions with the NFT Passport	14
Description of the biometric verification process	15
HASHBON PASS PROTOCOL	16
Protocol description	17
How the Hashbon Pass protocol works	18
Mandatory requirements for verifiers	19
Verifier rating	20
Social rating	23
Tokenomics	25
ISSUING LOANS IN DEFI	26
Loan security	27
Unsecured Loans (without collateral)	28
Credit rating	29
ENABLING SSI	30
What is SSI?	30
How SSI is applied in Hashbon Pass	31
COMPARISON WITH COMPETITORS	32
Key differences	33
HASHBON PASS ROADMAP	34
CONCLUSION	35

Welcome to the pages of the Hashbon Pass Whitepaper!

First of all, we want to introduce you to the Hashbon FiRe ecosystem and our mascot, the **HASH** raccoon.

In 2016, [Hashbon](#) was founded in the Czech Republic, providing the crypto market with two products – a cryptocurrency wallet and a payment gateway with 0% commissions for payment transfer processing. Hashbon's main task was to rethink the world of finance and reinvent its technologies, both in the centralized (CeFi) and decentralized (DeFi) sectors. In 2021, Hashbon launched a decentralized cross-chain bridge for token exchange as the [Hashbon Rocket](#) DeFi universe expanded to the Hashbon FiRe (Finance Reinvented) ecosystem.

The fuel and driving force of the ecosystem is [HASH](#) token, released in February 2021. This is a utility token issued on the following blockchains: Ethereum MainNet, BNB Chain, XDC Network, and Polygon Network. In the Hashbon FiRe ecosystem, HASH provides reduced fees within the wallet and payment gateway, pays premium rates within services and all token exchange transactions on the Hashbon Rocket platform. The mascot of the token and the Hashbon FiRe ecosystem has become the HASH raccoon, a purposeful and courageous traveler to new boundless worlds.

The HASH Raccoon will help you navigate the document and answer possible questions as you study the Hashbon Pass Whitepaper.





First of all, you may be wondering – what is Hashbon Pass and what purpose can it be used for?

Hashbon Pass, or **NFT Passport** by Hashbon FiRe is an NFT and a decentralized protocol for reusable identity verification on blockchains such as Ethereum, BNB Chain, Polygon and other EVM-compatible networks.

Our protocol involves the participation of three parties:

- ▶ Verifiers
- ▶ Users
- ▶ DeFi protocols that require user identification

The user's basic information is recorded on blockchain – nickname, citizenship and date of birth. Scanned documents and personal data are stored by licensed verifiers and are not accessible by third parties.

In addition to DeFi protocols, NFT Passport can be used for authorization on centralized exchanges (in customers' personal bank accounts), adult services (sites with restricted 18+ content), or as a much more convenient alternative to CAPTCHA.

The NFT Passport is issued by professional certified verifiers. Not only do they verify the authenticity of the submitted documents, but they also check the user's presence in lists of sanctions, PEP lists (Politically Exposed Person) or other black lists. Moreover, this information is updated even after the creation of the NFT.

Hashbon Pass' key feature is **anonymous KYC**. This means that DeFi-protocols do not actually have access to the user's personal data, but they can filter out individuals from sanction lists, as well as calculate the user's credit scoring and social rating.

Only the police or Courts, in the event of an investigation, may send an official request to a licensed verifier (which directly stores the user's personal data) in order to obtain the user's relevant information.

The problem of KYC in DeFi

Recently, the sector of decentralized finance (DeFi) has become much more popular. According to [DeFi Pulse](#), the DeFi market's TVL is \$94.41B (as of March 29, 2022), and [DeFi Llama](#) reports the total locked assets being at \$225.78B (excluding staking). This indicates that this sector's annual growth is reported to be approximately 200%. This – as expected – provoked a reaction from governmental agencies and state institutions that drew attention to the fact that DeFi services do not restrict usage of their services by criminals in any way, given that AML & KYC haven't been readily available in the sector.

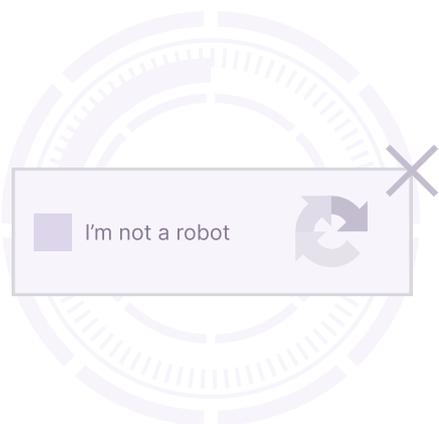
How exactly does the presence of an NFT Passport allow services to solve the KYC problem?



It's very simple: having an NFT Passport in conjunction with the approval of the verifier holds the user accountable for their actions when maliciously using DeFi services. In the case of financial fraud or other legal violations – when the police or other state officials are obligated to contact verifiers – they can get information regarding the identity of the offender. After that, it will be easy to hold the user liable via the judicial system on the basis of legislation, usage policy, etc.

The user can choose any licensed verifier with a sufficient level of trust and pass verification through them, allowing any smart contract to acquire information regarding the user's verification status, age and citizenship. If a user is placed under sanctions or has been blacklisted after passing verification, this information will be updated.

Spam protection and anonymous 18+ checks



CAPTCHA is an **ineffective** method of protection against bots, since AI and many manual recognition service can bypass it. Moreover, people consider CAPTCHA to be quite annoying. By making a request to verify the user's NFT Passport, the service understands that there is a person behind the screen, while the transfer of personal data is not carried out to services that aren't authorized to handle users' sensitive data.

Currently, 18+ verification services request a passport photo or a credit card from the user, however, not all users feel comfortable with breaching their anonymity when viewing 18+ content. An NFT Passport allows users to provide their age without revealing their identity.

Applications in the centralized sector



Among other things, NFT Passport can be used in classic centralized services – banks, exchanges, carsharing, etc., as a means of verification. Users will not need to repeat the verification process, while at the same time, their personal data is stored by licensed verifiers who have established themselves in the general Internet space as reliable data repositories.

How does NFT Passport work in the Centralized Finance Space (CeFi)?



When interacting with services that require identity verification, users will need to connect to the service's site via MetaMask or a similar wallet suitable for storing an NFT. Subsequently, the user will be verified by this specific service. At the same time, no personal data is shared with the service: the only information available to the given service is general data stored on the blockchain. This will ensure the safety of the user's sensitive data and address concerns regarding their personal information becoming available to third parties. User's information may not be displayed at all, there will be a green checkmark instead.

Anonymous KYC

Anonymous KYC?
Isn't that an oxymoron?

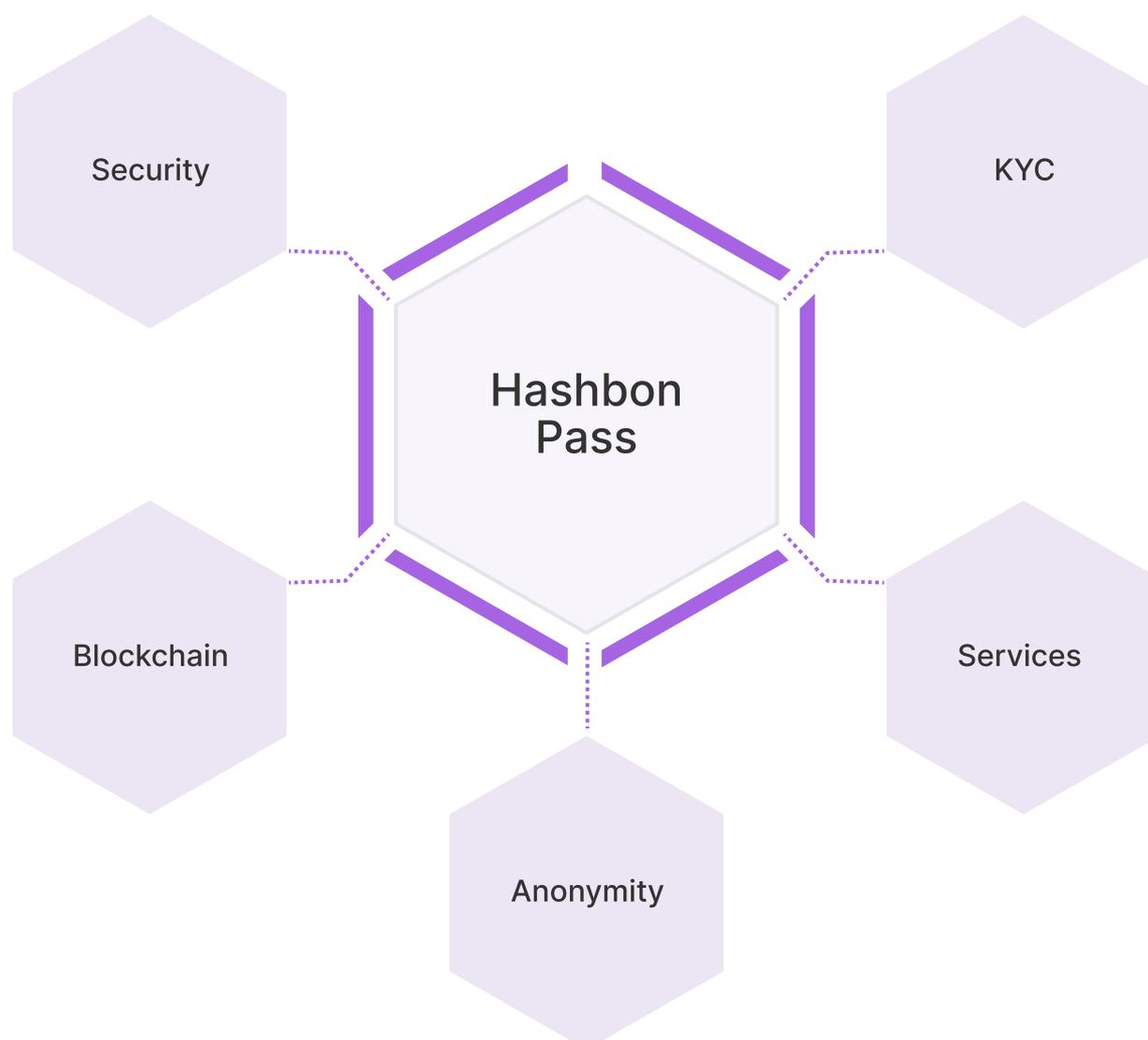


One of the recent most-discussed news that concerns anonymity is a [Facebook data leak in early April, 2021](#). We do not partake in speculation regarding the legitimacy of that specific incident or how it should have been treated. However, the very fact of a hypothetical possibility of data-leaks, services being hacked, or even the intentional transfer/sale of personal data is enough to demonstrate the need for an intervention, as the topic of data safety is important to us.

[The Hashbon Pass protocol](#) is the first ever [Anonymous KYC](#), through which DeFi services, including DEX, IDO, Play2earn, understand that they have a verified user active on their platform, determine their age, citizenship and also their presence on blacklists, all without having access to their personal data. At the same time, the user's personal data is stored only by licensed verifiers who issue NFT Passports. Such verifiers have licenses that comply with GDPR, which gives them the authority to work with clients' personal data.

Hashbon's vision of Anonymity and Security

Introducing the brand new product that compiles convenience and solidity while resolving KYC problem.



The Hashbon Pass open-source protocol assumes three groups of factors:

- ▶ **Licensed verifiers** – commercially licensed services, such as SumSub, OnFido, OnDato, which have the authority to work with user personal data
- ▶ **User** – any individual interacting with services
- ▶ **Service** – any DeFi protocol, that complies with AML & KYC policies

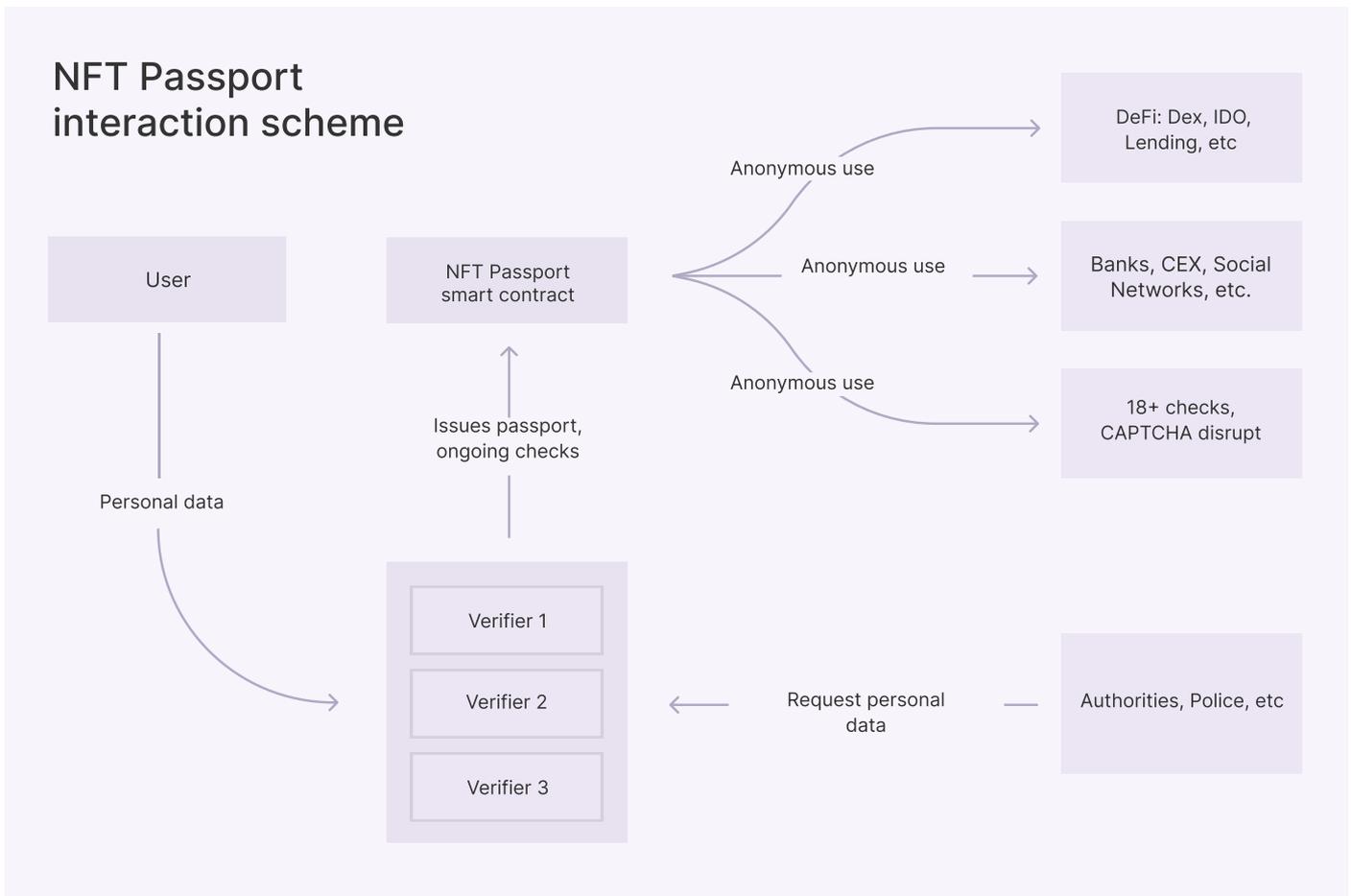
Anonymous KYC

All processes occur through the assignment of an NFT to each user

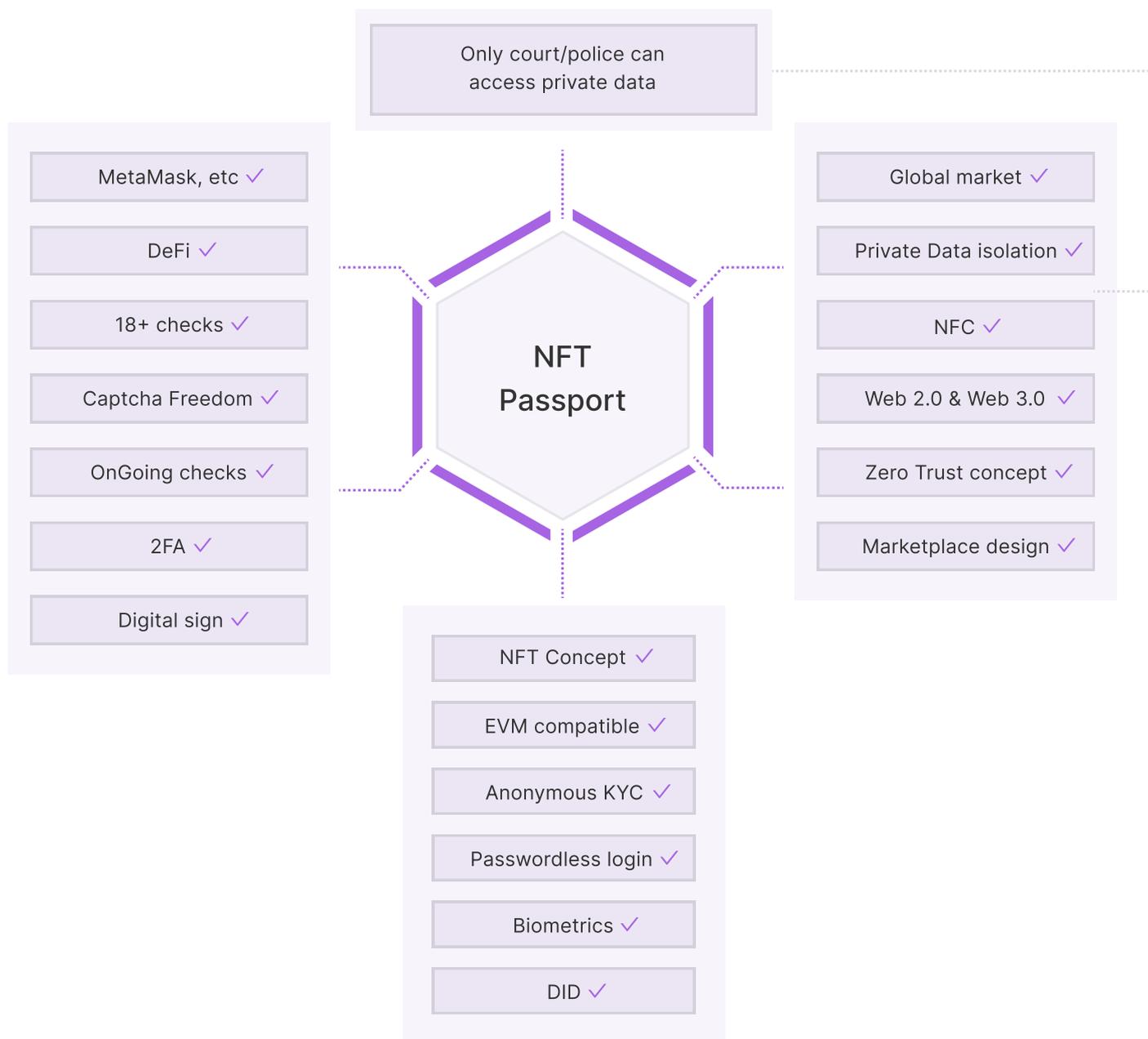


It is enough to get a passport, which in turn allows the user to be verified by one action via the site's integration of [MetaMask](#) or a similar wallet.

You can learn more about the applicability and processes of interaction between parties involved in the process of creating and using an NFT Passport from the diagram below:



Solution: NFT Passport



Hashbon Pass (Hashbon's **NFT Passport**) is an NFT. Each user can have several passports (depending on the validity period of their passports, as well as the presence of several nationalities). The passport can be transferred to another address, which has not yet been assigned to a certain passport. After the transfer of the passport has been completed, additional biometric verifications will be required.

Public Data of Hashbon Pass

What data is publicly available?



Data that is stored on the blockchain (and cannot be deleted):

- ▶ Nickname
- ▶ Date of Birth – at the request of the user
- ▶ Citizenship – at the request of the user

Data stored by licensed verifiers and is publicly available (it can be changed or deleted)

- ▶ Full name – in a masked manner (example: J**n S***h)
- ▶ Document type (passport, driver's license, ID card, etc.)
- ▶ Date of verification
- ▶ User's avatar
- ▶ Whether the verification has been successfully completed or not
- ▶ The cryptocurrency address for which verification has been completed (must match the user's address so that the passport can be trusted). The value of this field changes when the NFT Passport is transferred with the subsequent addition of the selfie
- ▶ Notes on the user's presence on PEP lists, sanctions and blacklists

Actions with the NFT Passport

What can a user do in a personal account with an NFT Passport?



Issue a new passport



Pass verification



Reissue the passport



Undergo additional checks
(for example, repeated selfies when handing over a passport)



Change the nickname



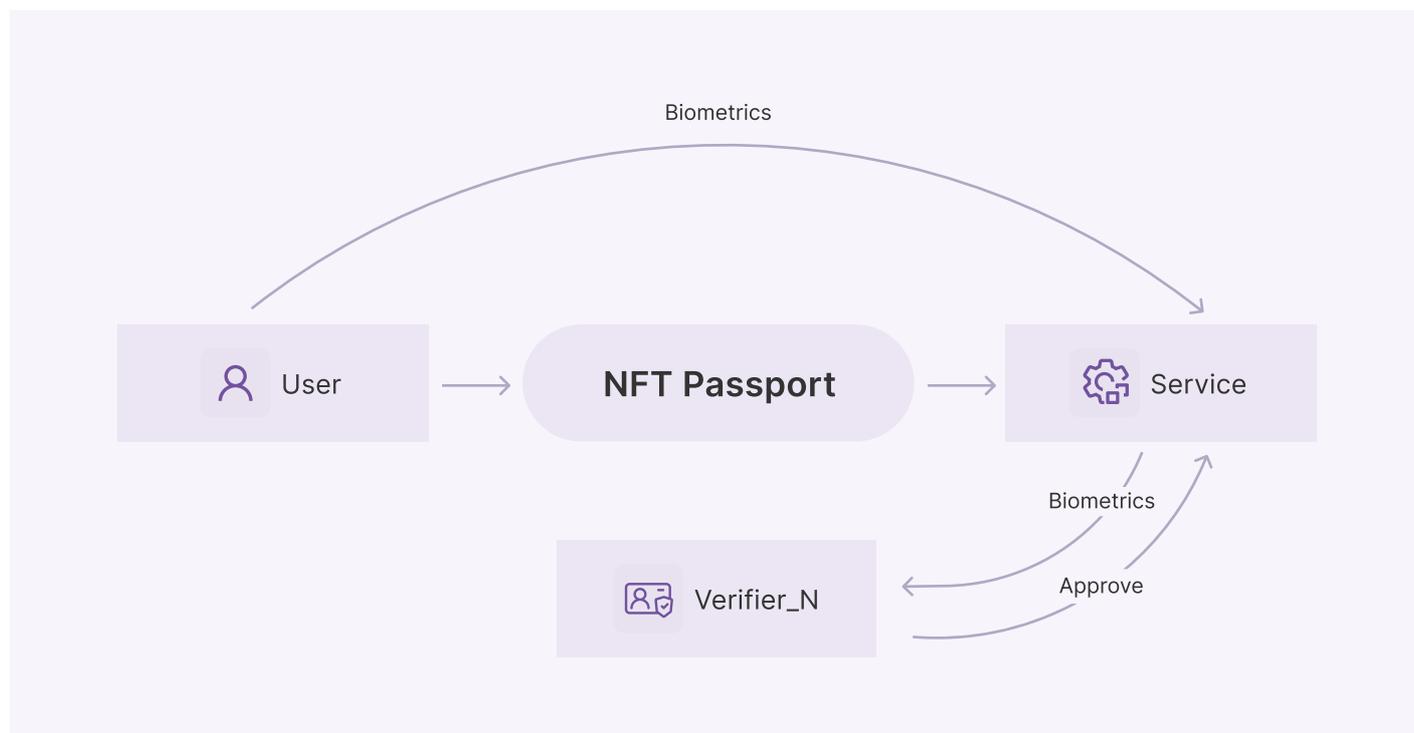
Burn the existing NFT Passport (delete)



Upload data (citizenship and date of birth) to the blockchain once for multiple following direct access to it via DeFi protocols

Description of the biometric verification process

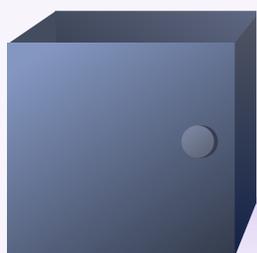
1. A user with an NFT Passport is verified by sending their biometric data to the service
2. The service, in turn, requests the verification status from the verifier
3. After confirming the identity, the user is provided with access to the service



Hashbon Pass Protocol

We are implementing a multi-blockchain solution, which is an NFT Passport that can be issued on all popular blockchains. Within the MVP's framework, the project will be implemented on Ethereum and the BNB Chain (those being the most popular in the field of DeFi), as well as on the Polygon network as a promising alternative to the main blockchains.

Where will the user's data be stored if the service suddenly needs access to personal data?



According to the protocol, the service provider initially trusts verifiers, and does not require direct access to personal data, which is why the protocol does not include the functionality of transferring user data without the user's authorization. If the service does not want to work with a verified user and intends to acquire their personal data on their own, their attempt will prove to be unsuccessful. Even the theoretical implementation of this functionality does not exist. Users should not worry about server-side data leakage.

Protocol Description

To begin, the user needs to be verified by licensed verifiers. Our protocol allows using various services via identity verification without publishing and sharing their data with the services themselves. The only required action on the user's end is to click on one verification confirmation button on the service's website.

The only thing a Hashbon Pass client has to do is to pass a one-time verification. Subsequently, only this user's nickname is stored openly on the blockchain upon the user's consent.

The client has to pay a fixed one-time fee (the fee will depend on the verifier itself, since different verifiers charge different amounts + it depends on the validity period of the user's submitted document). The money is used to pay for the verifier's service (one or more) and also to pay miners commissions (this will be explained in more detail in our Tokenomics). There will be no more payments, only if the need to reissue a new NFT Passport arises, for example, if the document used for verification expires.



How the Hashbon Pass Protocol works

Available licensed verifiers will be personally selected by the users themselves based on the verifier's rating. The rating, in turn, is based on a formula that calculates the degree of the verifier's trust (please refer to the "Rating of Verifiers" section below).

The user's data is stored by verifiers, which removes dependence on personal data storage by the service provider itself. The user's data is stored only by licensed verifiers for ongoing checks.



Using the Hashbon Pass ensures the users' full control over their own personal data. Services will not be able to get the users' data in any way.

In the event of fraud, the service can contact the police and other government agencies that investigate criminal activity, but the service itself does not have any means of accessing the users' personal data without police intervention. This is a very important standard of our NFT Passport – complete anonymity and security of users' personal data.

This is the most important feature and paradigm of NFT Passport by Hashbon – 100% anonymity and personal data security.

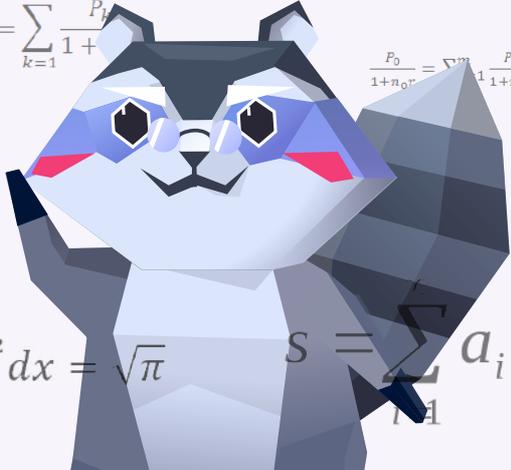
Mandatory requirements for verifiers

- ▶ Compliance with security standards set by the protocol developers
- ▶ Refusal to provide personal data to third parties, except for official appeals by state agencies – police, court order, etc. (forced disclosure)
- ▶ Compliance with laws regarding storage of personal data, including GDPR and other applicable legislation

Verifier Rating

For mutually beneficial cooperation between the user and the verifier, we have created a special evaluation system that is constantly displayed online. This system determines the rating of each individual verifier and assigns it a confidence coefficient. It is advantageous for the user to trust verifiers who do their job the best and it is important for the verifier to gain the trust of users and thereby increase their profit through commissions.

How is the verifier's trust rating calculated?



$$Q = \frac{\pi}{4} \int_0^l d^2 dl.$$

$$\int_{-\infty}^{+\infty} e^{-x^2} dx = \sqrt{\pi}$$

$$S = \sum_{i=1}^n a_i$$

$$\frac{P_0}{1+n_0 r} = \sum_{k=1}^m \frac{P_k}{1+n_k r}$$

$$\frac{P_0}{1+n_0 r} = \sum_{k=1}^m \frac{P_k}{1+n_k r}$$

Verifier Rating

The criteria and calculation formula are as follows:

k_i — the coefficient of importance of each given parameter in our rating (the larger it is, the greater the contribution made by the corresponding indicator of the verifier)

x_i — the indicator of the verifier in the i -th segment according to Hashbon's estimate

Criteria	Their coefficient (k is estimated from 1 to 5)
Time to check the information to acquire the verified status	3
What documents a verifier accepts for verification	3
Security of clients' stored personal data	5
Percentage of verification errors	5
History of data leaks	5
User votes from the same region	3
User votes from the other region	1

$$NonNormScore = \sum_{i=0}^n k_i \cdot x_i$$

where x_i is calculated from 1-10 points

Verifier Rating

After calculating the points received, we normalize the data to the maximum value possible, so that it is more convenient for users to work with the assessment.

$$Max = 10 \cdot \sum_{1}^{10} k_i = 270$$
$$Score = \frac{NonNornScore}{Max} + (D)^*$$

* - In the future, when working with verifiers, we will monitor the indicators and enter the variance D to take into account all possible shortcomings in the verifier's evaluation.

Social Rating

The **NFT Passport** opens the door to creating a social rating, which gives new opportunities and conveniences for interactions on Web 3.0. Each holder of an NFT Passport will have their rating calculated based on communication with other users.

For this rating, the ability to write reviews and comments for each user/service has been added. Upon passport issuance, the user can view accounts of other verified participants and draw conclusions: whether they should interact with any given user or not. This creates an opportunity to evaluate other users' reputation, assess their interests and improve on the likelihood of a perfect social interaction.

Also, the ability to filter out inappropriate comments and reviews, as well as users, if necessary, will be built into our interface. A social rating doesn't rely on one sole indicator to form a user's status, a social rating is multidimensional.



In the future, we plan to add a neural network that checks the social rating alongside our operational system structure. This will allow the user to determine user-friendly content in advance, and in turn, speed up the process of filtering out unnecessary news and finding people with similar views.

Social Rating

This scoring provides:

- ▶ If the users do not want to see comments and reviews of an opposing view, then they can change the necessary fields of visibility of certain views in their extension settings.
- ▶ It is easier and more convenient for the user to find relative content they need or other users with similar interests. This will allow them to quickly and seamlessly be integrated in their users groups.

Reducing aggression on the web by restricting the content of other views. It is a scientifically proven fact that online users are much more aggressive towards other views, although in real life these indicators are much less prevalent. Our system allows users to bring their internet environment as close as possible to their real lives, where aggression is drastically minimized

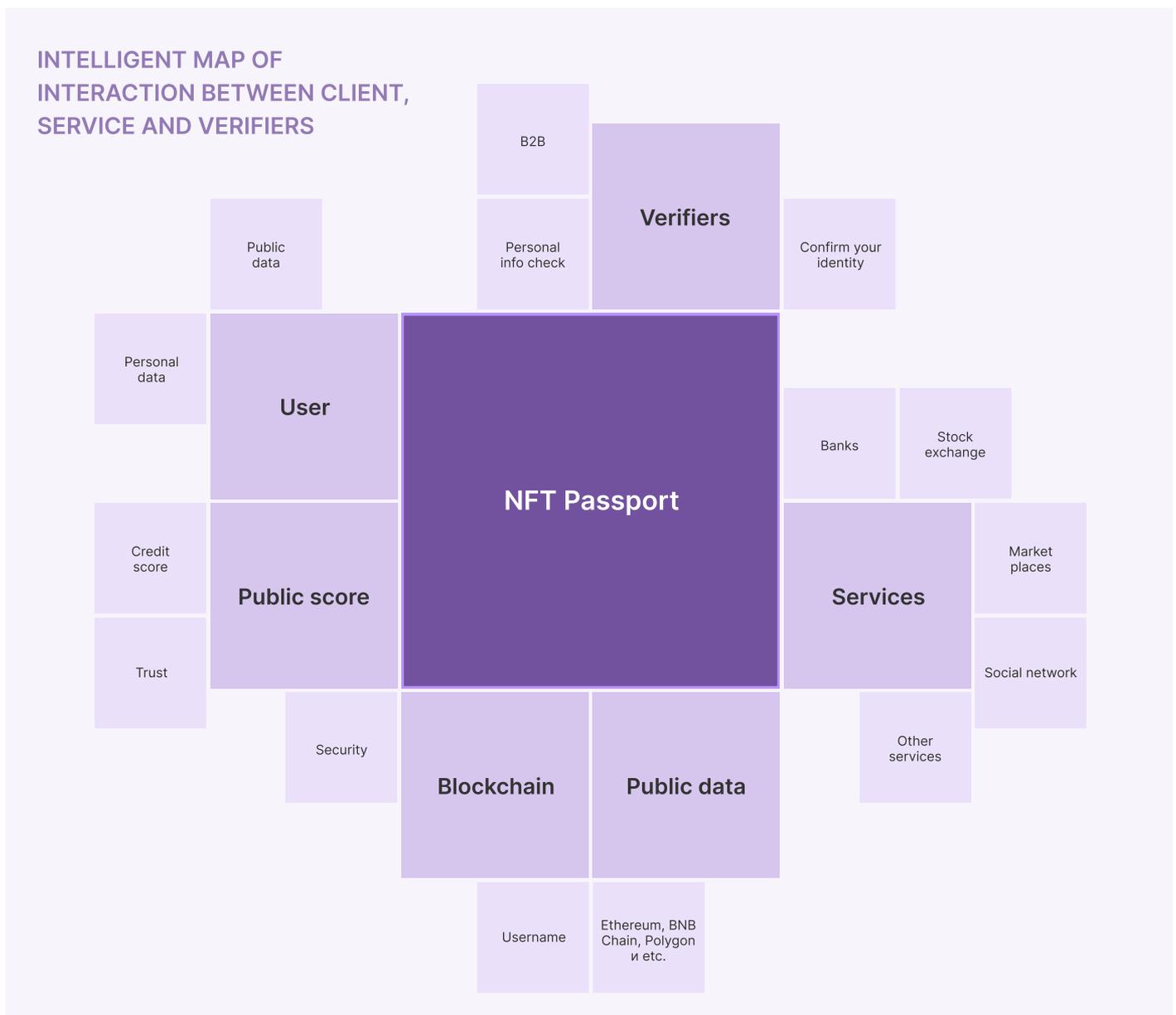


Tokenomics

At the time of issuing an NFT Passport, the user is charged a commission, which is distributed as follows:

- ▶ Payment verifiers' fees
- ▶ Payment of the network and miners' commission
- ▶ A portion of the commission will be used to buy back HASH tokens from DEXs, with subsequent distribution as a reward among stakers on Hashbon Rocket

When submitting a request to change the data in an NFT Passport, users will also need to undergo a biometric check, for which a fee will be charged.



Issuing Loans in DeFi

DeFi loans are already very popular due to their accessibility, simplicity and economic attractiveness for both borrowers and lenders. Thanks to these loans, the user can receive additional funding from deposits without dealing with banks or any actual counterparties. Stock traders can take out quick loans, increasing trading leverage.



<https://www.defipulse.com>

Loan security



How secure are DeFi loans?

DeFi lending is quite secure, since users do not store their funds on the platform, and all transactions are carried out through open source smart contracts, this way, the process of lending and borrowing in DeFi becomes transparent and secure, however, only to the extent that smart contracts themselves are transparent and secure.

That is why **code testing by an independent audit is a standard for all DeFi projects.**

Unsecured Loans (without collateral)

At the moment, collateral loans have become widespread in DeFi. There is a concept of flash lending (without security), but this is not a loan in the general sense of the word, because at the moment of approval you need to make a deposit that fully covers the loan amount. This scheme is safe but makes no sense, since the client does not receive any extra amount.

For the effective implementation of unsecured loans, it is necessary to introduce the concept of identity into the blockchain, as well as credit scoring. Identity on the blockchain will be a guarantee of creditworthiness, ensuring that the user is responsible for all their actions.

The [Hashbon Pass](#) protocol helps solve this identity problem and opens the door to creating a decentralized credit rating.

Credit Rating

The key element for solving the identity problem on the blockchain is the **NFT Passport**. The verified user is checked for criminal records, sanctions, PEP and other blacklists, which, without a doubt, increases the level of trust towards him/her and reduces lending rates.

Credit scoring can be calculated based on modern practices of international financial institutions, which at the moment are an excellent indicator of the actual credit ability of the borrower. The rating can consist of the following components: application-scoring, collection-scoring, behavioral-scoring, fraud-scoring. Such a system will allow users to quickly be integrated with already well-known credit agencies, and also allow credit bureaus to tap into a new sphere - the blockchain. Such a rating opens up new opportunities in the field of DeFi applications and will allow a substantial number of potential customers and services to enter this field.

A credit rating built on the basis of modern standards in the field of lending will avoid the risks of non-payment of debt and additionally reduce interest rates. Moreover, user verification significantly reduces the risk of issuing a loan to untrustworthy borrowers.

Enabling SSI

Taking into account current trends, we understand that some services, due to their specifics and the legislation of their respective countries, cannot use an anonymous model such as Hashbon Pass. Of course, we expect community support in the future in promoting the concept of anonymity in DeFi, but for now, for the user's convenience, we are embedding additional functionality in the form of SSI.

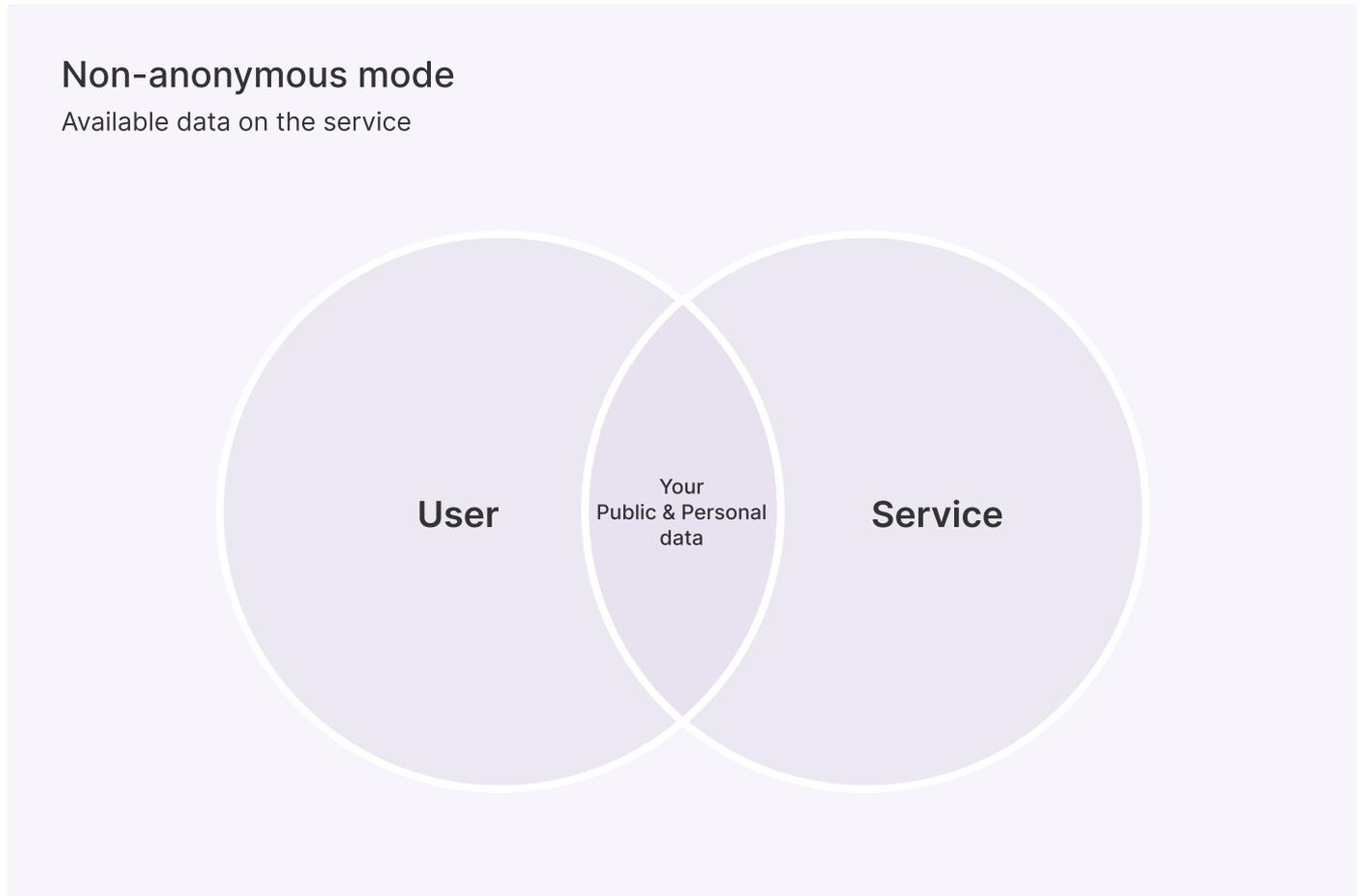
What is SSI?

[Self-Sovereign Identity, SSI](#) — SSI is a set of information regarding an individual. This information can be managed by the user and shared with any private individuals or public institutions. Additionally, access to this set of information can be revoked at any time at the user's will.

The SSI system is based on a decentralized technological architecture and is designed to prioritize security, privacy, individual autonomy.

How SSI is Applied in Hashbon Pass

With SSI functionality activation, personal data can now be transferred to services, but strictly with the user's permission.



This approach provides convenience, as data can be sent between the user and the service without the participation of a verifier (verifier can be enabled, if necessary). In this case, the data will be encrypted with a public key, which allows only the user and the service to have access to the provided information.

Comparison with Competitors

A study of the crypto project market and an analysis of three competing companies that are working on blockchain identity was conducted. All projects are under development and - at the time of preparation of the study in March 2022 - are not actually used live anywhere in DeFi protocols. Below is a list of competitors and a comparison table:

- ▶ Kilt: www.Kilt.io
- ▶ ONTO ID: www.Onto.app
- ▶ Identity Verification by Civic: www.Civic.com (www.Identity.com)

Signs	Hashbon Pass	Kilt	Civic (Identity)	ONTO ID
Application of NFT technology	✓	✗	✗	✗
Compatibility with popular DeFi protocols	✓	✗	✗	✗
Support of popular wallets (MetaMask, etc)	✓	✗	✗	✗
Support of multiple verifiers	✓	✓	✗	✓
The possibility of passing verification in the moment	✓	✗	✓	✓
Plans to enable credit scoring	✓	✗	✗	✓
Number of installations	0	4000+	1000+	15 000+
Has a funny raccoon character	✓	✗	✗	✗

Key differences

- ▶ One of our key concepts – the use of the **NFT standard**. None of the listed competitors make use of this technology.

What benefits does this provide?

Support for all –without exception– crypto wallets that support the storage of NFT. This opens the door to a multi-million audience and a very rapid adoption of the technology. All of these competitors work exclusively through their own wallets, which greatly limits them and their users. For example, [one of the popular browser-based crypto wallets MetaMask has 30 million users \(as of March 16, 2022\)](#). Our NFT Passport can be loaded into MetaMask precisely in 1 click.

- ▶ All our 3 competitors work on their own blockchains, which makes it impossible to integrate them into modern DeFi.

Hashbon Pass is released on a number of popular blockchains such as Ethereum, Binance Smart Chain, Polygon, and other EVM-compatible blockchains. This means that **our protocol is very easily integrated into all popular DeFi protocols**.

Roadmap Hashbon Pass

Q2 2022	Launching the Hashbon Pass MVP
	Publication of the Hashbon Pass specification for the integration of client services
	Improving the design of users' personal account and website
	Pitching and launching partnerships with developers of DeFi protocols
Q3 2022	Connecting 2-3 KYC providers
	Adding Biometrics
	Verifier ratings
Q4 2022 – 2023	Releasing open source code of software for verifiers
	Development of a mobile application and browser extensions
	Social rating
	Credit rating

Conclusion

Our **NFT Passport** is an up-to-date, innovative, and a previously non-existent solution to the KYC problem in DeFi for both individual and commercial use (B2C & B2B). Both services and users, together with verifiers, will stand to benefit from Hashbon Pass. This is a completely new approach to the issue of anonymity and security.

With the help of our NFT Passport, users will be able to use a huge number of services without the transfer of any personal information. The world and technology are moving forward, and Hashbon Pass will allow people to keep up with the times. It's time for real anonymity without additional risks of personal data leakage. Only Hashbon Pass allows you to plunge into the new world of Web 3.0, feeling absolutely protected, from both users and services. All participating parties will benefit from utilizing the capabilities of our protocol.

Conclusion

When developing the project, we at Hashbon were guided by the principles that have become fundamental for our team, developed in the process of working on our previous projects and tasks, namely:

► Innovation

In 2021, we launched a cross-chain bridge and the Hashbon Rocket DeFi platform, about which [Investing.com](#) wrote: *"In light of Hashbon Rocket's unique value proposition, users will be able to swap an ERC20 token for another token that is compliant with the BEP20 standard and vice versa while creating liquidity pools."* It was a trail-blazing solution in its field and in turn, it paved the road for partnerships with other DeFi players.

► Customer orientation and security

Hashbon React was included in the [top 10 payment gateways of 2021](#) according to [Yahoo Finance](#): *"Hashbon takes care of the KYC and AML requirements. In under 5 minutes, buyers/consumers can scale the identity verification process and become eligible to buy products or pay for services with cryptocurrencies"*.

► Openness and transparency

In the last two years, we have gathered a community of over 30 thousand crypto enthusiasts from all over the world; we held an ICO in which 338 people supported us and we raised over \$921K USD. Every week we share reports highlighting our activity on [Medium](#), and more than 40 people in our team are open to communication on LinkedIn and [Telegram](#) – the project's community channel.

If you have any inquiries or additional questions regarding Hashbon Pass, we will be happy to answer all of them:

- General inquiries: info@hashbon.com
- Partnership requests: bd@hashbon.com
- Media inquiries: pr@hashbon.com

HashbonPass



Telegram
[@hashbon_com](https://t.me/hashbon_com)



Reddit
[/r/hashbon](https://www.reddit.com/r/hashbon)



Twitter
[@hashbon](https://twitter.com/hashbon)



Medium
hashbon.medium.com

