Synk

LitePaper

Abstract

The cryptocurrency ecosystem continues to face an increasing number of attacks, such as Drainer-as-a-Service (DaaS) and scams, which pose a significant threat to users' security.

This paper proposes Synk, a lightweight solution that provides secure remote instances of the most common crypto tools, shielding users from malicious actors while maintaining the convenience of using web-based services.

Introduction

The cryptocurrency market is rapidly growing, making it increasingly attractive to cybercriminals who utilize various attack vectors like DaaS and scams to exploit unsuspecting users. To protect users, we propose a lightweight solution that utilizes remote instances of popular crypto tools hosted on trusted servers. These instances will be securely accessible via the web through an intuitive, user-friendly interface.

Problems

As cryptocurrency users and asset owners, we have identified several new threats within our sector. We are likely to be faced with multiple security threats such as:

1

Private key theft:
Users' private keys are the keys to their digital wallets. If attackers steal these, they have control over your funds. This theft could occur from keyloggers, phishing attacks, or brute force attempts.

2

Wallet hacking:
Online crypto-wallet services can be compromised by hackers. In such cases, your private keys might be stolen, or you may lose access to your wallets if the service goes out of business or shuts down.

3

Cryptocurrency Scams and Frauds:
Fake ICOs (Initial Coin Offerings) or exchanges are scams where fraudsters dupe investors into giving away their cryptos. Scammers may also impersonate reputable entities like blockchain projects, exchanges, or even government agencies to steal cryptocurrency from users.

4

Cryptojacking:
Malware secretly uses your computer's resources to mine cryptocurrency without permission. It can significantly reduce a computer's performance and incur additional power bills. Phishing Attacks: Phishers might create fake websites or use social engineering tactics to deceive you into providing personal information, wallet addresses, private keys, or other sensitive data.

5

Lack of User-Friendliness in Wallets/Platforms:
A poorly designed wallet interface may lead users to accidentally send their funds to wrong addresses (often due to incorrectly copying and pasting address codes), lose their private keys, or face difficulty managing multiple cryptocurrencies in a single wallet.

6

Loss of Seed Phrases or Passwords:
If you forget your seed phrase (a collection of randomly-ordered words) or password, you may never be able to recover access to your cryptocurrency wallet.

These threats, already well identified in the crypto ecosystem, are gaining in power every single day, with the appearance of malicious actors offering DaaS.

We also note that in the case of an advanced, potentially exposed user, he or she could encounter doxing risks. Our solution proposes to enhance user's OPSEC.

Solution

The solution aims to be fully encrypted, meaning:

1. Users data is encrypted at rest using users seed.
2. User activities are protected on transit using network security solutions.
3. User remote instance random access memory is encrypted using his seed.

Using a remote workstation allows you to use crypto assets even on untrusted devices.

Our proposed solution, Synk, consists of the following aspects:

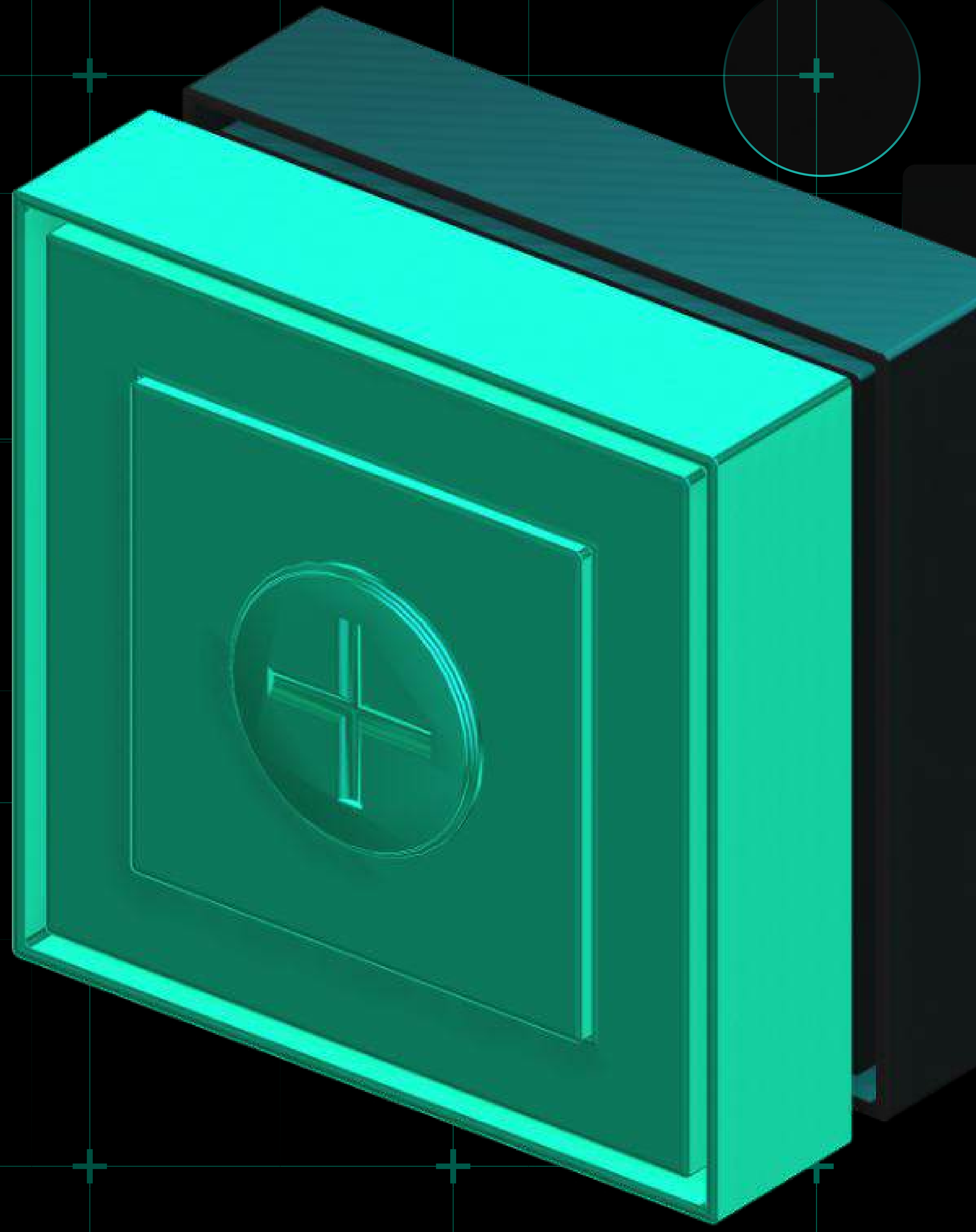
Network Security

Tor

We will give you the ability to navigate through Tor to avoid pirates and other malicious threat to observe your traffic. It will guarantee a better security while navigating on the Web and keep your data safe at any given time.

VPN

We will set up a VPN for you to connect to it and with Tor make your connection even more robust and secured.



System Hardening

- Application security: We will make sure that any apps used on our system is trustable and well configurated so you can use it without any fear of your data being leaked or compromised.

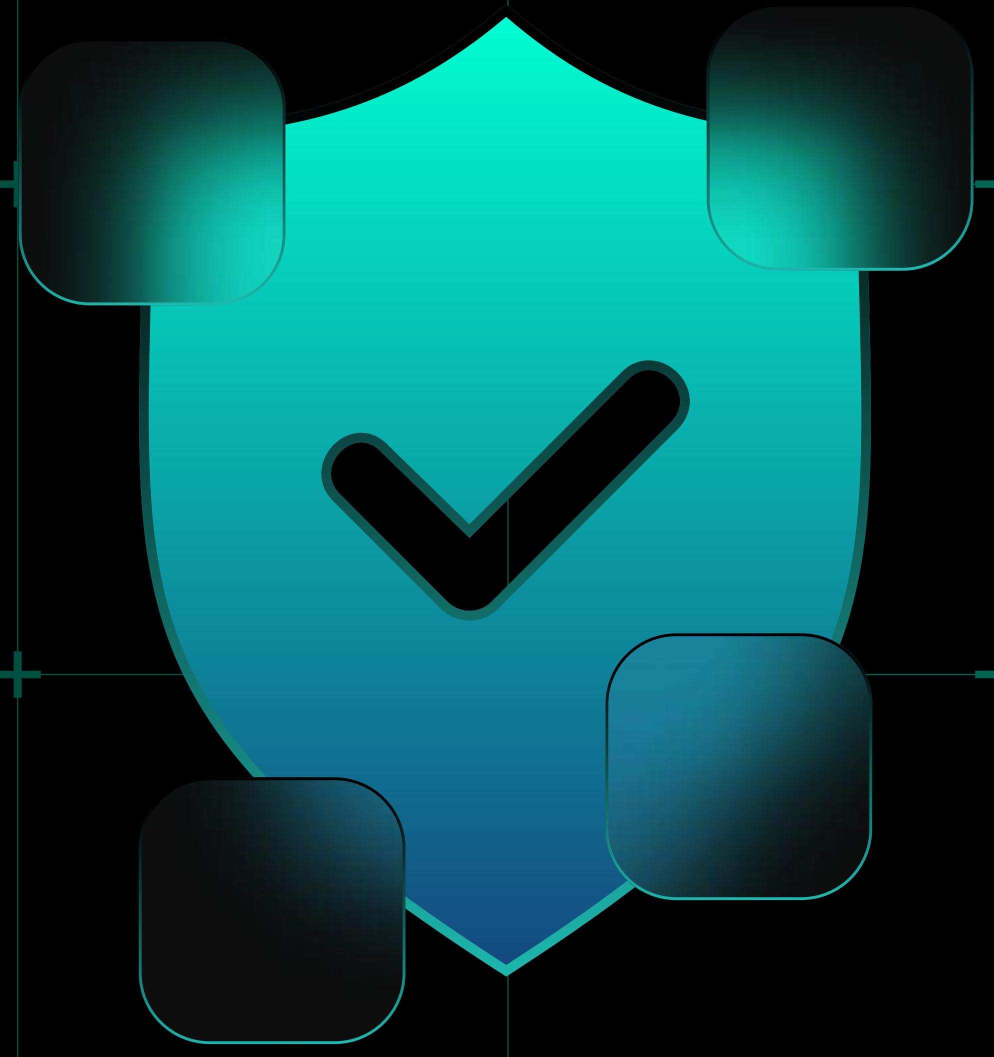
- Deep network security: Network security is a real threat nowadays and a lot ‘Man in the middle attacks’ are being conducted by malicious hacker. However, there are ways to prevent this, and we will ensure that hackers cannot gain access remotely by employing in-depth network security layers.

- Smart activity analysis in local using advanced detection algorithm issued from.

- Packaging of the solutions in containers to leverage confidential computing (on-the- fly RAM encryption).

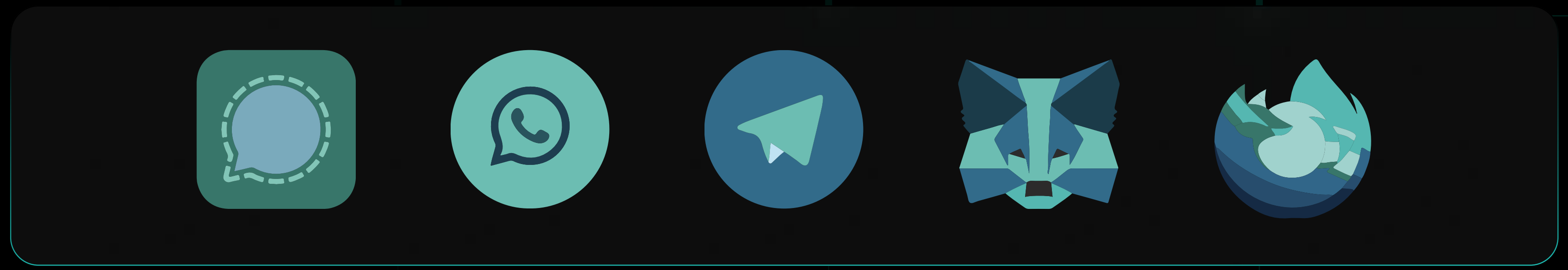
- Multi-level threat detection (application, operating system & platform).

- Safe file opening using DangerZone like software that sanitizes untrusted files.



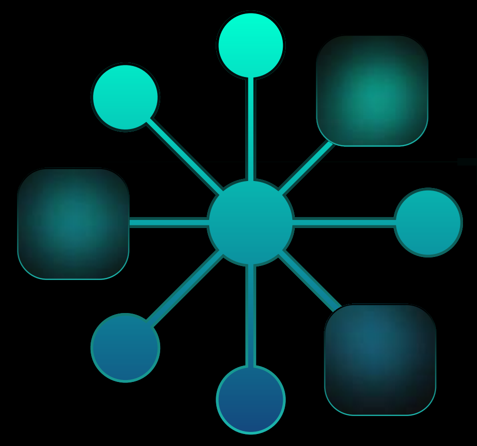
Providing the Tools

We intend to provide as many applications as you need for your daily tasks.. At the beginning here is a basic list of the applications we intent to provide:



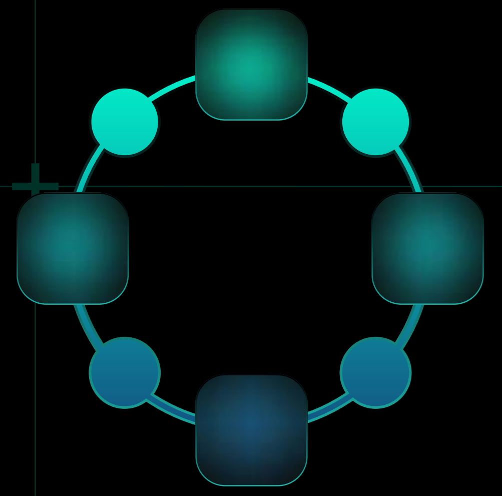
Data Persistence and Security

The OS, as it is designed, deletes all of the files you have set on the computer so that there is no trace of it. We will however provide a data persistence offer that will let you store in our databases your files.



At first, centralized

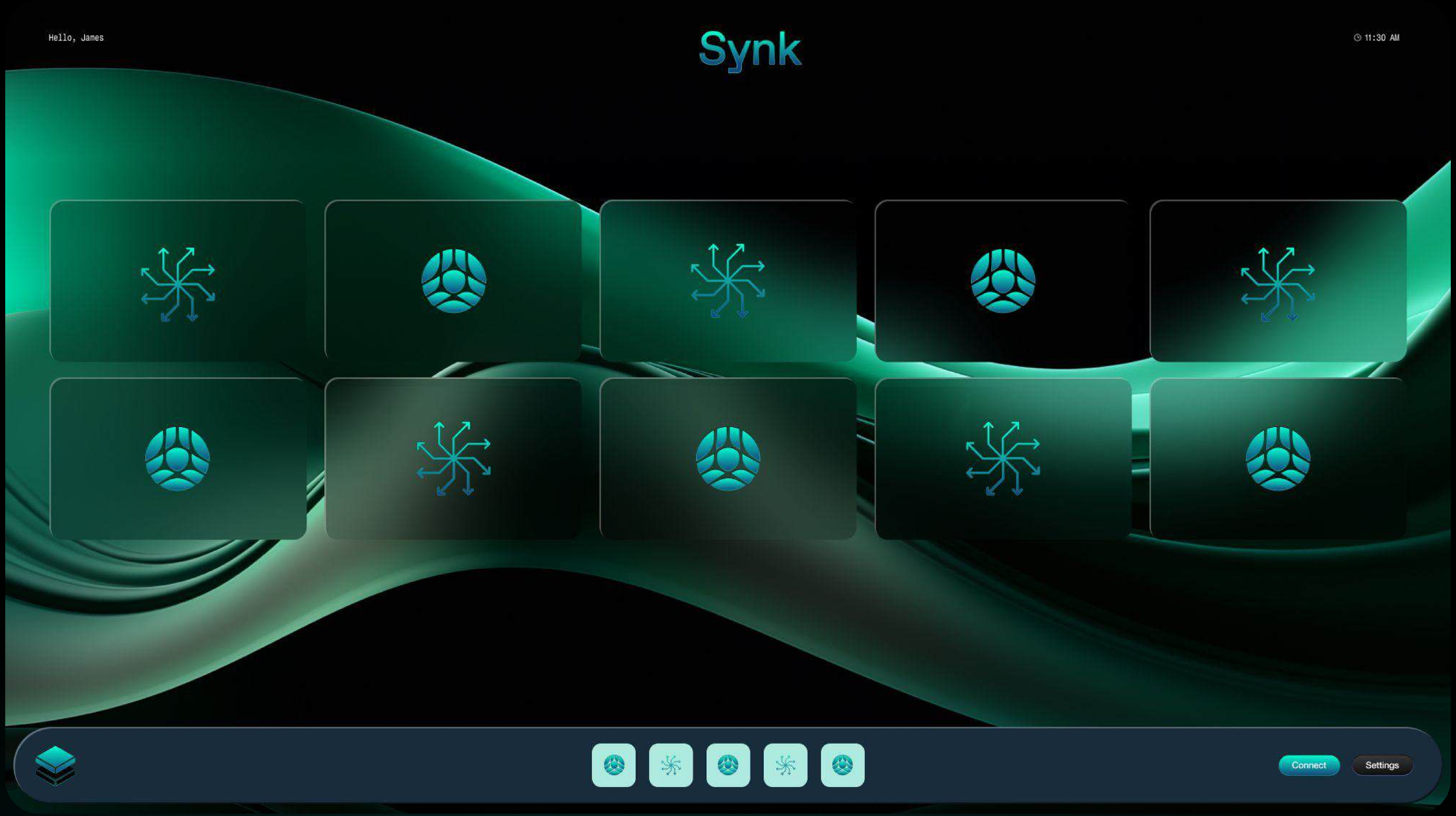
To reduce the time to market of our solution, we propose it to be partially centralized on the storage aspect. At first it will be centralized and well secured on our servers so that there are none leaks of it. This will give you a space where you can store any data and consult it anywhere in the world, but it will also guarantee you that your data are safe and sound. This kind of storage already exists online but we will make your data compatible with our OS and only accessible by you.



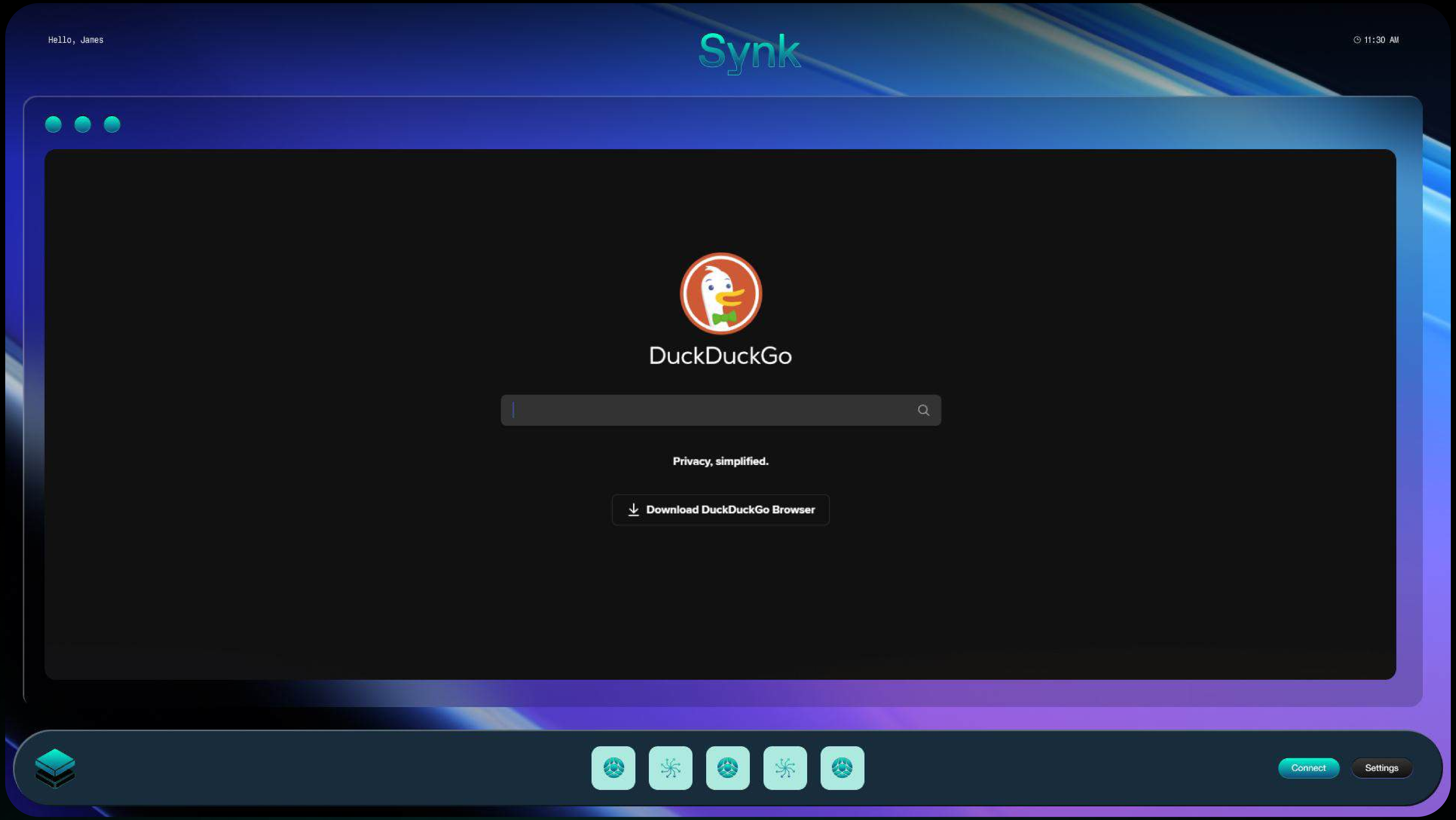
And then, decentralized

Following our studies and implementation of proof of concepts on decentralized storage solutions, we will migrate all users data to a decentralized storage solution. Our current projection is based on the use of IPFS and the pinning mechanism. It will be even faster for you to access your data and make them even safer and unreachable by potential threats.

DAPP UI



DAPP UI


Hello, James
Synk
11:30 AM
DuckDuckGo
Privacy, simplified.
Download DuckDuckGo Browser
Connect
Settings

$SYNK Utility

ACCESS TO SYNK WORKSPACE

$SYNK, an ERC20 token on the Ethereum blockchain, is essential for accessing Synk's secure environment. Users will need to hold $SYNK to unlock various services and tools within the Synk ecosystem.

SYNK STORE

Synk offers an internal store where users can install new applications on their OS. Certain resource-intensive applications may require payment in $SYNK, either directly or through the staking system, to offset infrastructure costs. This includes access to application packs such as a browser pack, or a messaging pack containing apps like Telegram, WhatsApp, Signal, and others. Additional packs will be made available through our application hub, offering even more options for customization.

SYNK CONFIG

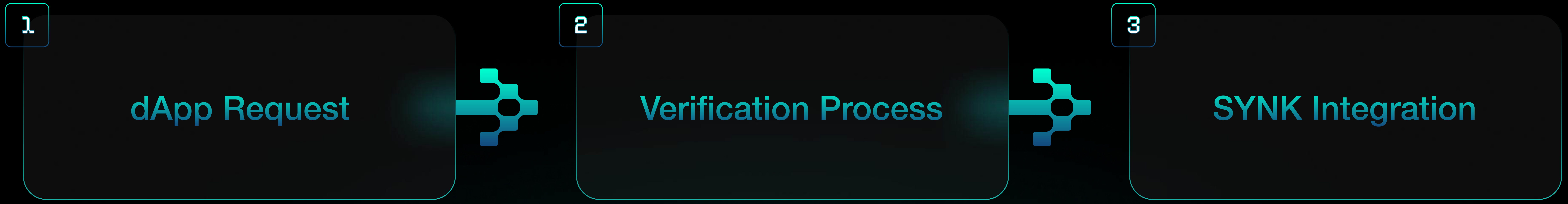
For advanced users, Synk provides deeper OS customization. This includes the option to select decentralized VPN providers, configure network exit nodes by country, and personalize the interface through texture packs to modify the theme, all driven by community involvement or staking of $SYNK tokens.

STAKING REWARDS

Holders of $SYNK can stake their tokens to earn rewards, promoting long-term holding and reducing market sell pressure. These rewards further incentivize user engagement within the ecosystem.

$SYNK dApps for Growth and Revenue

Synk offers a B2B service that allows projects to add their dApps to the Synk store. Projects can submit a request, undergo full verification by our team, and pay in ETH for integration. This process supports Synk's growth, while a portion of the revenue is distributed to $SYNK token holders.



1 dApp Request

2 Verification Process

3 SYNK Integration

Roadmap

1 Q3 2024 →

Token release

Staking contract release

Closed alpha of XXX product, then free open alpha of the product to gather reviews from the community

2 Q4 2024 →

Releasing product v1, with a focus on security and privacy with basic tools, centralized

Tools pack 1 (crypto tools), tools pack 2 (osint tools)

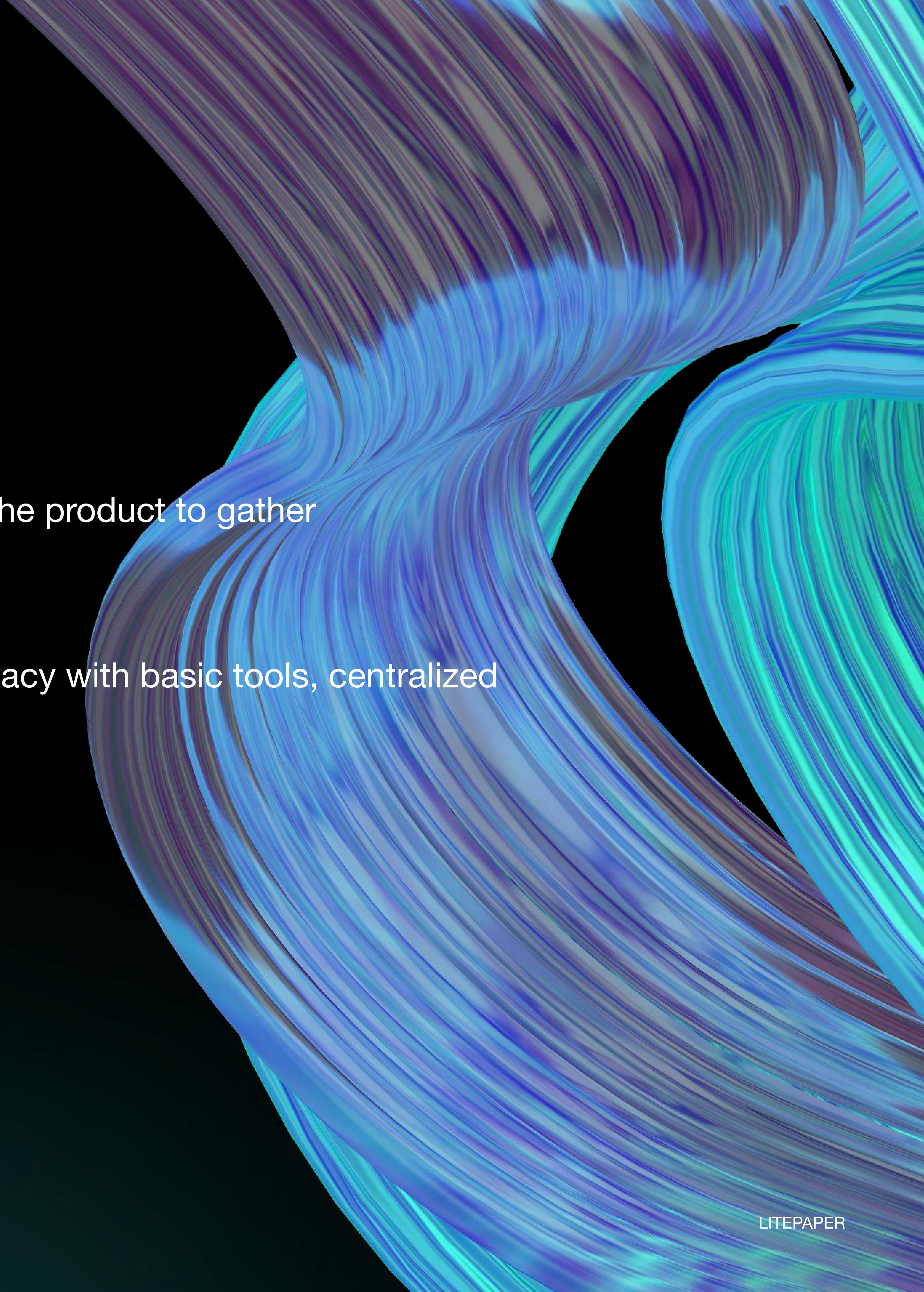
Security audit, labeling and certification

3 Q1 2025 →

Enabling data decentralization of Synk

4 Q2 2025 →

Fully working Operating System



References

Mandiant Blog

Hundreds of Thousands of Dollars Worth of Solana Cryptocurrency Assets Stolen in Recent CLINKSINK Drainer Campaigns
https://www.mandiant.com/resources/blog/solana-cryptocurrency-stolen- clinksink-drainer-campaigns

Sentinel One Blog

The Rise of Drainer-as-a-Service | Understanding DaaS https://www.sentinelone.com/blog/the-rise-of-drainer-as-a-service-understanding-daas/

Wikipedia

Confidential Computing
https://en.wikipedia.org/wiki/Confidential_computing