LITE PAPER

LEGAL DISCLAIMER

This Whitepaper is intended to explain the new cryptographic digital token called CYVO whereby the tokens shall be used by the CYVO community to access various kinds of products and services provided on the CYVO Digital Ecosystem.

Please note that CYVO tokens are not meant to constitute securities in any jurisdiction. These are utility tokens in their nature. This Whitepaper does not intend to constitute an offer of buying securities or a solicitation for investment in securities in any jurisdiction.

This Whitepaper is for informational purposes only and does not contain any recommendations or advice to sell or purchase CYVO tokens or products and services. It does not constitute any investment decision or contract which means that this document cannot be the basis for an investment or concluding an investment agreement. CYVO products are only for the objective purposes as contained herein.

You agree and acknowledge that if you are a citizen or resident of any jurisdiction where cryptocurrencies are banned or restricted either partially or completely, you shall not purchase any CYVO tokens.

Any information provided in this Whitepaper has not been approved or checked by regulatory bodies and authorities. Publishing and distributing this Whitepaper does not mean that it has complied with the laws, regulatory requirements, rules or regulations of any applicable jurisdiction.

EXECUTIVE SUMMARY

CYVO is developing a series of revolutionary solutions for problems related to data privacy through the use of post-quantum encryption processes and integrating within its ecosystem blockchain-based cryptographic tokens called “CYVO”.

CYVO tokens are revolutionary in the way that users can trade them specifically for the goods or services that shall be offered by CYVO.As a company, CYVO is developing an ecosystem through its platform, on which its users will regain control over their data through various products such as the ‘World's Most Secure Laptop’, ‘Secure Browser with revolutionary communication channels, ‘VPN’ ‘Next Generation Quantum Encrypted Digital Wallet’ and ‘Stealth Encrypted Cloud Storage’. These products and services can all be purchased using CYVO tokens.

Our team of [150] developers include some of the world’s leading minds in encryption technology. Our products are several generations ahead of anything in the market and have been subject to rigorous testing by third party firms comprised of former intelligence officers from some of the world’s foremost intelligence agencies. The result: Unbreakable, Unhackable, Secure & Private.

1. THE NEED FOR A SECURITY SOLUTION THAT PRESERVES YOUR PRIVACY & PROTECTS YOUR FREEDOM

There's no such thing as privacy online. You are being watched. Your every keystroke and clicked hyperlink leaves a trace. However, it's not just out there, somewhere; it's recorded, analyzed, and interpreted. Your life is woven into the fabric of the digital world. The question is who is watching? Who knows your likes, dislikes, vices, perversions, political views? Who knows the intimate details of your relationships? Who knows your secrets? Who knows you better than you know yourself?

Privacy is a myth. Privacy is dead. The erosion of civil liberties began a long time ago, and you had no idea it was happening. We will discuss the backdrop in the context of the United States, but the same narrative applies globally. Let's start the timeline in recent memory with a shocking abuse of political power a mere 20 years ago.

The Patriot Act increases the governments surveillance powers in four areas:

1. **Records Searches.** It expands the government's ability to look at records on an individual's activity being held by a third parties (Section 215).
2. **Secret Searches.** It expands the government's ability to search private property without notice to the owner (Section 213).
3. **Intelligence Searches.** It expands a narrow exception to the Fourth Amendment that had been created for the collection of foreign intelligence information (Section 218).
4. **"Trap and Trace" Searches.** It expands another Fourth Amendment exception for spying that collects "addressing" information about the origin and destination of communications, as opposed to the content (Section 2140)

2010: The Rise of the Internet of Things

You Home is Tapped - Are Your Devices Spying on You?

From internet-connected televisions, toys, fridges, ovens, security cameras, door locks, fitness trackers and lights, the so-called "Internet of Things" (IoT) promised to revolutionize our homes. IOT evangelists routinely heralded a hyper-connected future, where everything from your refrigerator to your tea kettle would be connected to the Internet. The end result, they promised, would be unprecedented convenience and a Jetsons-esque future, contributing to a simpler, more efficient existence. The end result wasn't quite what was advertised.

What this could potentially mean is that someone could, for example, hack into a household's wi-fi network & collect data from IoT devices. It might be as simple as knowing when lights are switched on to determine when a home can be burgled. Someone with more malicious intent could turn on your oven while shutting down smoke alarms and sensors.

May 2013: Edward Snowden Reveals the NSA's Surveillance Dragnet

Every Aspect of Your Life Exists in A Database

"Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say." - **Edward Snowden**

Snowden, the most famous whistleblower of a generation, gave thousands of classified NSA documents to journalists Glenn Greenwald and Laura Poitras. The documents showed in great detail how the post 11/9 intelligence apparatus was collecting data in bulk on American citizens and people around the world through programs like PRISM, XKeyscore, LoveINT, and a host of others. The revelations showed that the NSA had backdoors into the databases of many of Silicon Valley's largest companies, that it was surveilling world leaders and American allies, and that the U.S. government's surveillance state had become ever present in American life.

August 2013: Hackers Steal the Data of 3 billion Yahoo Users

Centralized Data is Vulnerable and Subject to Attack

In September 2016, as the company attempted to sell itself to Verizon, Yahoo belatedly revealed it had been the victim of a series of major hacks in 2013 and 2014. After initially claiming that 500 million users were impacted, it would later acknowledge that the hack impacted roughly 3 billion users, , the biggest data breach in U.S. history. Yahoo would ultimately have to pay a $35 million penalty to the Securities and Exchange Commission for pretending the hacks never happened, and another $80 million as part of a class action settlement. But as with most "punishment," much of the money went to lawyers, and the penalties paled in comparison to the money made from monetizing user data.

March 2017: The Equifax Hack Heard Around the World

Your Government Turns a Blind Eye to Consumer Protection

The last decade saw no shortage of breaches that exposed mountains of personal data, be it the hack of Marriott (500 million customers), Adult Friend Finder (412.2 million users) or eBay (145 million). But none highlighted corporate incompetence or government fecklessness quite like the 2017 hack of Equifax, which exposed the financial data of 145 million Americans. In part because data would later reveal that Equifax knew about the

vulnerability and did nothing about it. But also, because the punishment doled out by the FTC—which included a $125 cash payout that disappeared when consumers went to collect it—showcased a feckless government incapable and unwilling to seriously rein in corporate America's incompetence and greed.

2018: Facebook Lets Cambridge Analytica Abuse Your Private Data

Your Data is Being Used to Manipulate and Control You

While Cambridge's abuse of Facebook data was first reported in 2015, it wasn't until 2018 that people realized the full scope of the problem. For years Facebook casually allowed third-party app-makers unfettered access to consumer datasets, allowing outfits like Cambridge to weaponize your personal information in the lead up to the 2016 election.

2019: Wireless Carriers Busted Selling Your Cell Phone Location Data

They Know Where You Are at All Time

Thanks in no small part to Congress' decision to kill FCC broadband privacy rules in 2017, there's been little penalty for telecom giants that abuse your private information. Case in point: Motherboard's blockbuster January, 2019 investigation showing that wireless carriers routinely sell your every waking movement to a wide variety of often dubious middlemen.

2020 Onwards - COVID-19 sparks upward trend in cybercrime With workers outside the 'castle walls' of their companies, criminals have it easier

Ransomware has long posed a cybersecurity threat to companies and infrastructure, but experts say the problem has exploded in recent years due to COVID & work of home adaptability. Last year was especially egregious, with ransomware victims in the US paying out nearly $350m, according to the global security group the Institute for Security and Technology – a 311% increase over 2019. The FBI's Internet Crime Complaint Center has released its annual report that includes information from 791,790 complaints of suspected internet crime—an increase of more than 300,000 complaints from 2019—and reported losses exceeding $4.2 billion. The above alarming statistics are reported just out of the US. The global data is further alarming .

SOCIAL MEDIA USE AROUND THE WORLD

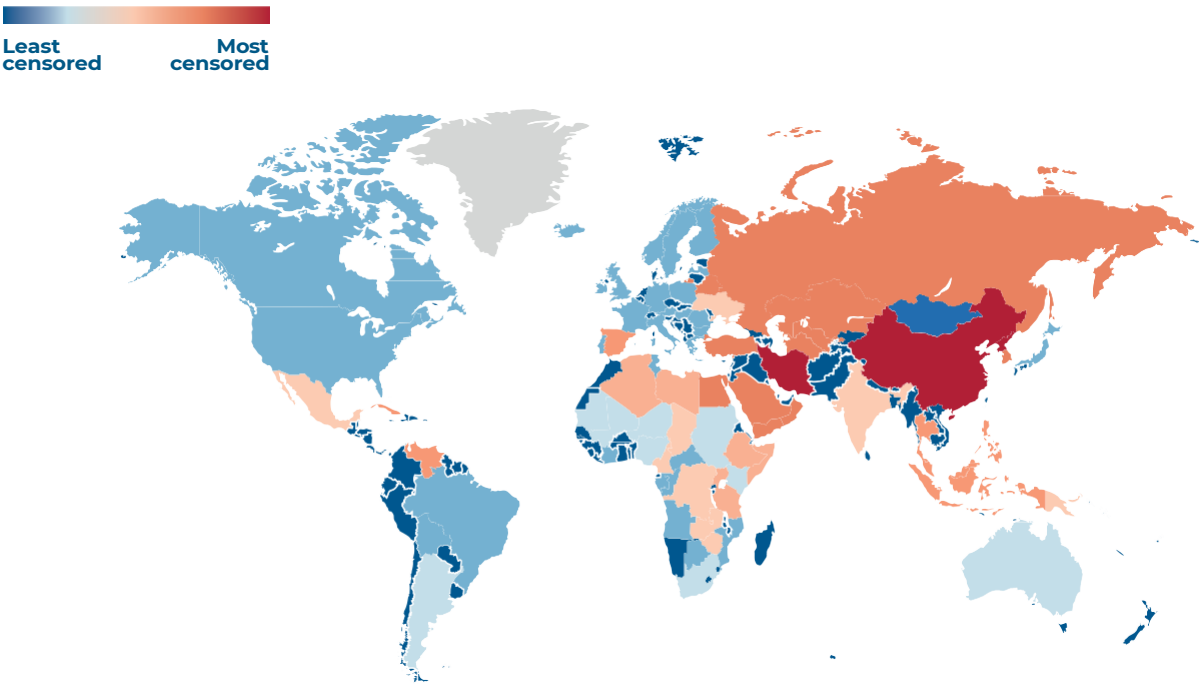
USE OF SOCIAL MEDIA NETWORKS AND MESSENGERS SERVICES, WITH DTAIL FOR MOBILE SOCIAL MEDIA USE
SOCIAL MEDIA USER NUMBERS MAY NOT REPRESENT UNIQUE INDIVIDUALS

TOTAL NUMBER OF ACTIVE SOCIAL MEDIA USERS	SOCIAL MEDIA USERS AS A PERCENTAGE OF THE GLOBAL POPULATION	ANNUAL CHANGE IN THE NUMBER OF GLOBAL SICOAL MEDIA USERS	PRECENTAGE OF SOCIAL MEDIA USERS ACCESSING VIA MOBILE PHONES	AVERAGE AMOUNT OF TIME PER DAY SPENT USING SOCIAL MEDIA
4.48 BILLION	**56.8%**	**+13.1%** +520 MILLION	**99.0%**	**2H 24M**

Global Social Media Users

With ongoing restrictions and pending laws, our online freedom is at more risk than ever. But where in the world can citizens enjoy equal and open internet access – if anywhere? Typical impingements on freedom of access include restrictions or bans for torrenting, pornography, social media, messaging/VoIP apps and VPNs, and restrictions or heavy censorship of political media. Although the usual culprits take the top spots, a few seemingly free countries rank surprisingly high.

Which countries are the most censored in the world?



Most Censored Countries for Internet Access

Section 230 is a provision of the 1996 Communications Decency Act that protects companies that host user-created content from lawsuits over posts on their services. The law shields both internet service providers, like AT&T, Comcast and Verizon, and social media and internet platforms, like Facebook, Instagram, YouTube, Twitter and Google. The law provides social media companies with sweeping protections that let them choose what content they restrict, and how. This means social media platforms can't be sued for taking down content or leaving it up.

By eliminating liability risk, Section 230 has allowed companies to experiment. Without it, Twitter and Facebook almost assuredly wouldn't exist, at least not as they do now. Most of the problems around Section 230 involve which posts social networks allow to stand and which ones they remove.

As the rhetoric around Section 230 has heated up, lawmakers on both sides of the political aisle have introduced a flurry of legislation over the past year. Some call for liability protections to go away entirely, while others want to alter or refine the protections. Other bills entirely strip away liability protections and would have companies earn those

The bottom line is free speech is no longer free. It comes at a price, especially if your views are non-conforming to the accepted and politically-mandated narrative. Persons with views counter to the dogma-of-the-day are simply de-platformed. It seems truth is a matter of perspective. As a result, your news is scripted and debate is no longer tolerated. Welcome to 1984, the Orwellian Future where the Ministry of Truth is governed by Big Tech.

Conclusion

Your life has been reduced to a data set. The freedoms and rights you take for granted have been chipped away, and you had no idea. A string of faceless enemies have been created to justify the passage of invasive laws. Do you think it stops here?

At CYVO we believe that your individual liberty and freedom is sacrosanct. You are the sacred master of your own domain. Our ecosystem is designed to give you back control of your autonomy. You may not be able to fight the creation of the mousetrap, but you can stop yourself from tasting the cheese.

What side of history will you fall?
To your freedom.

2. PROPRIETARY SOLUTIONS IN DEVELOPMENT BY THE COMPANY

Securing your data and privacy is an immense challenge. The strength of your privacy solution is only as strong as the weakest link. A single vulnerability can compromise your entire privacy solution. That's why CYVO is creating a series of solutions that fit seamlessly together to provide its users with unparallel security and peace of mind.

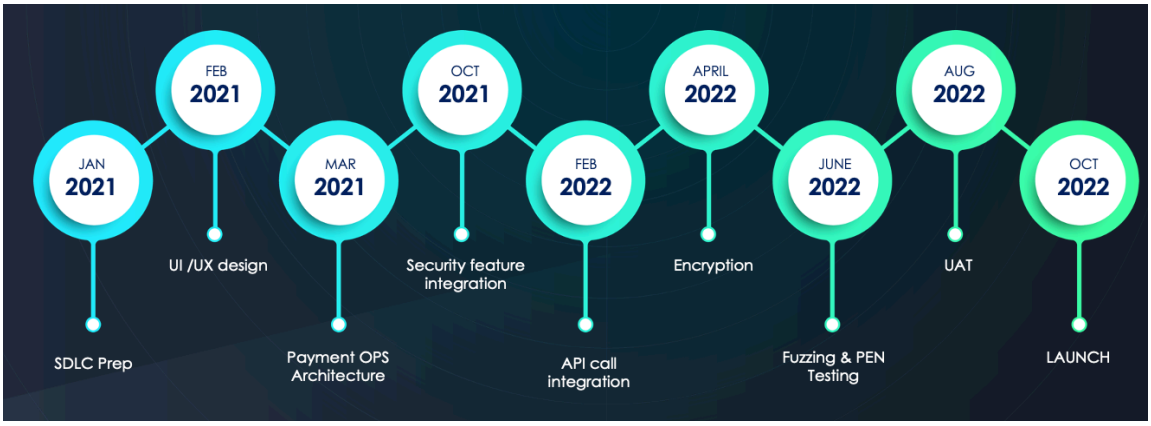
The Company offers a suite of certain super-secure, user-friendly, fail- proof, unhackable, untraceable products and services such as the 'Ultra-secure OS', 'Secure Browser with revolutionary communication channels, 'VPN' 'Next Generation Quantum Encrypted Digital Wallet' and 'Stealth Encrypted Cloud Storage'.

(i) Ultra-secure OS

The Company also offers the world's most secure OS which runs a unique secured operating system and has many features as shown below.

- User data including messages and media are encrypted end-to-end with post quantum encryption
- MAC address changes every time you re-connect to Internet
- Designed from the ground up with center measures to thwart any form of intrusion
- Physical key Login-Ultra secure 2 factor security with credential challenge
- Custom OS dose not allow any third party apps or root access
- Custom application suite for essential software>s like Spreadsheet, e-mail, chat, Tor Browser
- Multi-tiered access control with self-destruct mechanism at each stage
- Secure decentralized ultra secured storage
- Full disk encryption
- Cache System flashes after every session
- Inbuilt super-secure Encrypted VPN

CYVO Laptop Features



(ii) VPN, Secure Browser and Revolutionary Communication Channels

The Company is also planning to offer a super-secure, user-friendly, fail- proof and cost efficient VPN, Secure Browser and Revolutionary Communication Channels in Stage 2. The timelines for these products/services have not been decided as yet.

Security

Clear browsing data
Control site and content access
Password manager
"Do not track" with browsing requests

Extensions/Plugins

Supports Chrome extensions

Tabs & Windows

Private windows and tabs
Auto unload

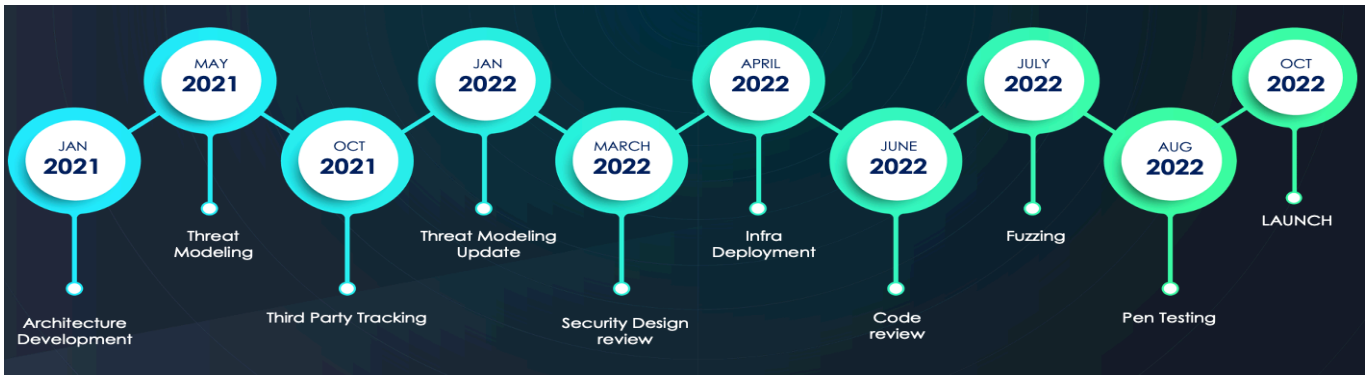
Shields

Block ads
Cookie control

Firewall Protection

Encrypting user activity
Block trackers across all apps
Protect all connections
Data protection

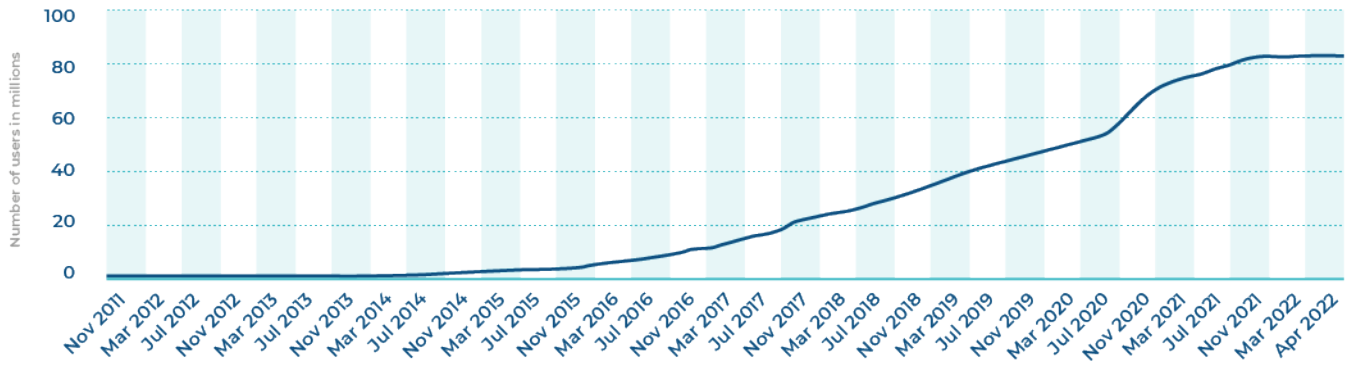
CYVO Web Browser Features



CYVO Web Browser Development Timeline

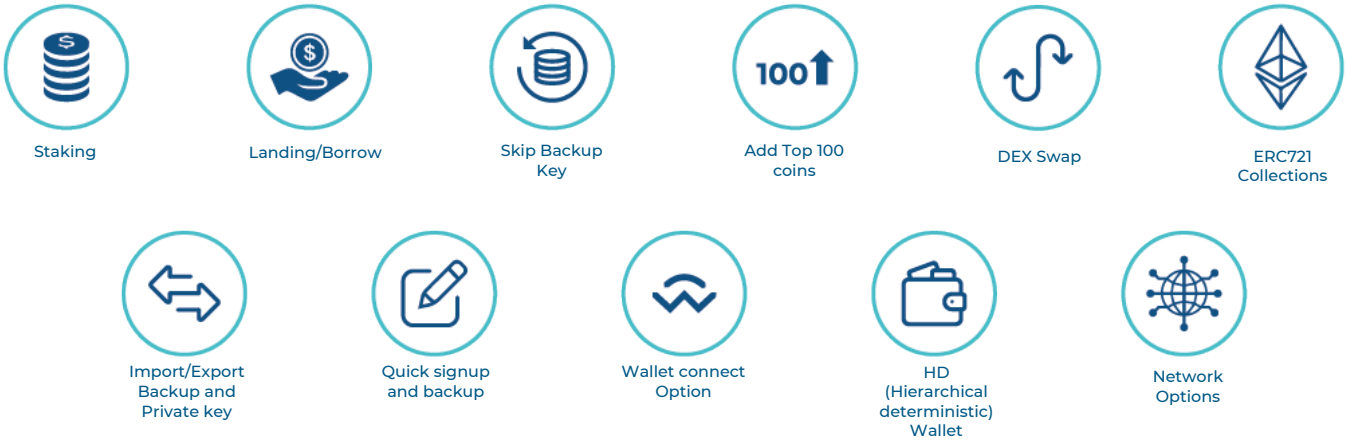
Next Generation Quantum Encrypted Digital Wallet

How many Bitcoin wallets are there? Blockchain.com wallets, something that makes purchasing Bitcoin possible, reached over 82 million wallet users at the end of April 2022. User figures for multiple cryptocurrency apps worldwide grew significantly, as is revealed when comparing download figures from the Coinbase, Blockchain Wallet, Crypto.com, BRD, Trust, Luno, Binance, Bitcoin Wallet, Bitcoin Wallet by Bitcoin.com, and Coinbase Wallet app

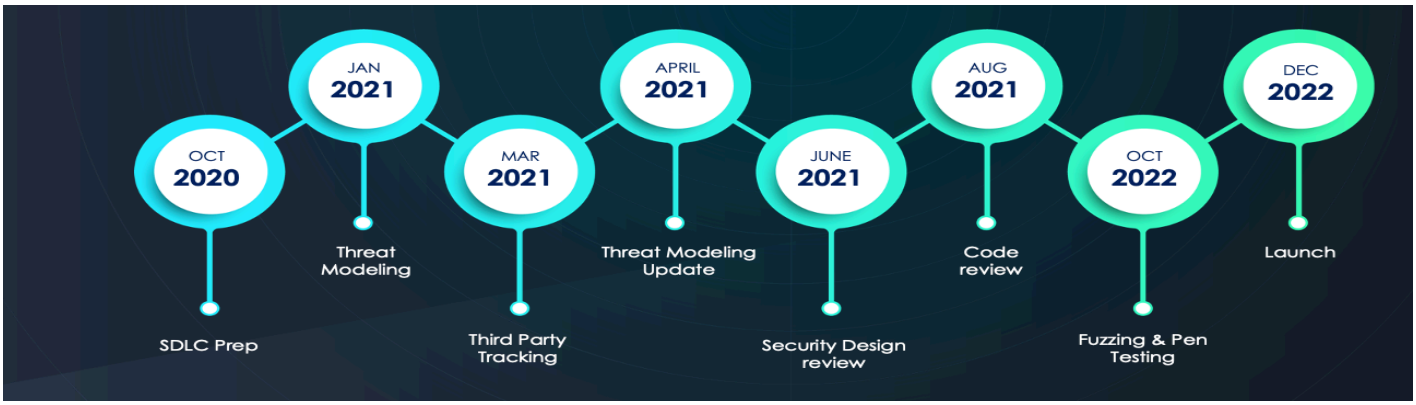


Number of Blockchain Wallet Users Worldwide

Exact user figures for Bitcoin are not available, but it is estimated that the global user base of all cryptocurrencies increased by nearly 210 percent between 2018 and 2022. The increase in demographics might have been caused by both a rise in the number of accounts as well as improvements in identification. More accounts in exchanges or wallets became systematically linked to an individual's identity, which made it easier to estimate the minimum user numbers associated with accounts on each service provider.
The Company is developing a super-secure and user-friendly Wallet for the next generation of cryptocurrency which is supported by its highly secure architecture and many features including, without limitation: multi -factor authentication, multi-tiered encryption, pattern sniffing protection and TOR network support to mask IP address and location.



CYVO Wallet Features



CYVO Wallet Development Timeline

(i) Decentralized Stealth Storage

The Company offers ultra-secure, fail proof, un-hackable, untraceable and anonymous decentralized stealth storage designed to keep you in control of your data. The storage has many features including, without limitation - privacy, security, durability, cost efficiency and reliability.

ANONYMOUS STORAGE

IPFS based decentralized architecture using Code obfuscation and encryption to ensure no data can be traced to the originator unless intended to by them.

INDUSTRY LEADING SECURITY

Blockchain enabled using cybersecurity frameworks, assurance services and best practices to reduce risks against attacks and fraud.

PRIVACY

Your data can only be read by you using the custom multifactor authentication process.. The platform in essence only facilitates and secures the exchange of node based data packets.

DURABILITY

Highly cost efficient as cost to host is distributed across multiple regions and geographies.

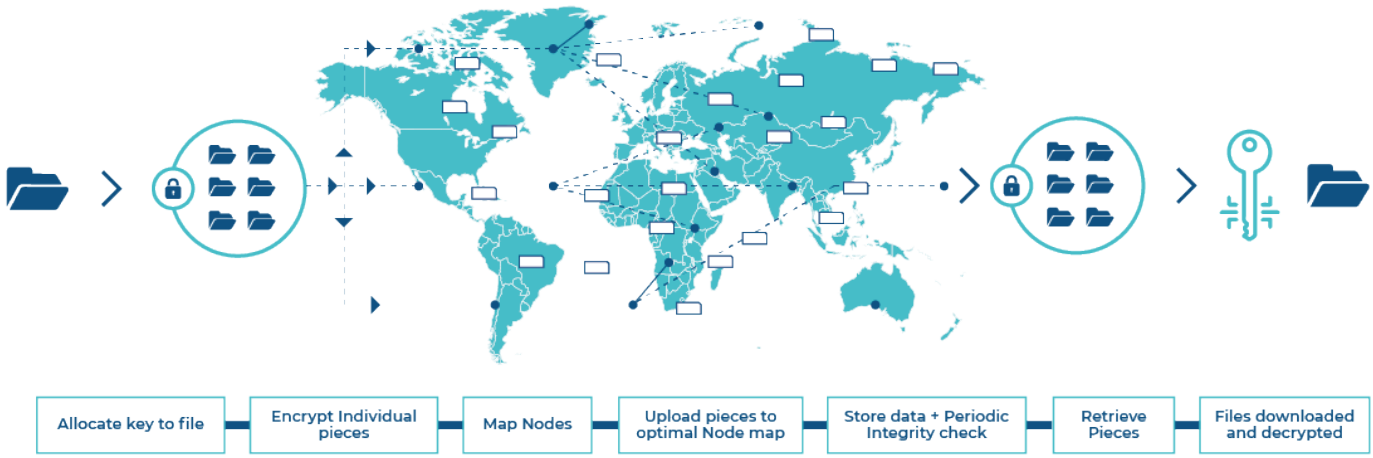
COST EFFICIENCY

Highly cost efficient as cost to host is distributed across multiple regions and geographies.

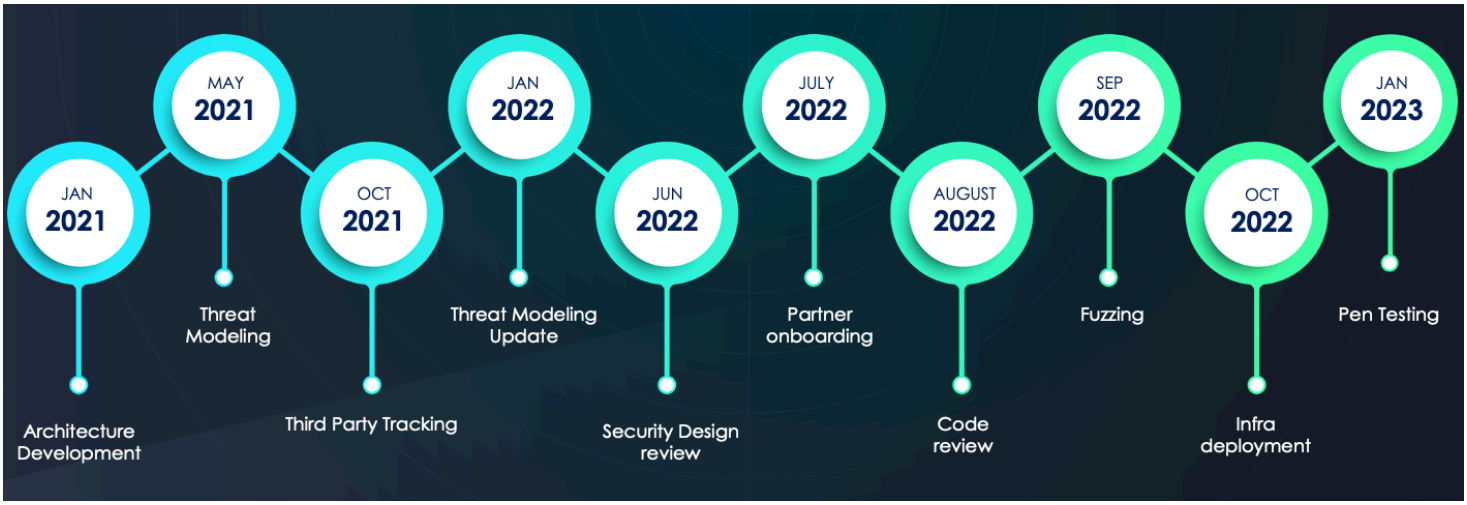
RELIABILITY

At any given point your data is hosted and stored only in nodes that have met the minimum criteria and have been vetted to ensure robust support.

CYVO Storage Features



CYVO Storage Functionality



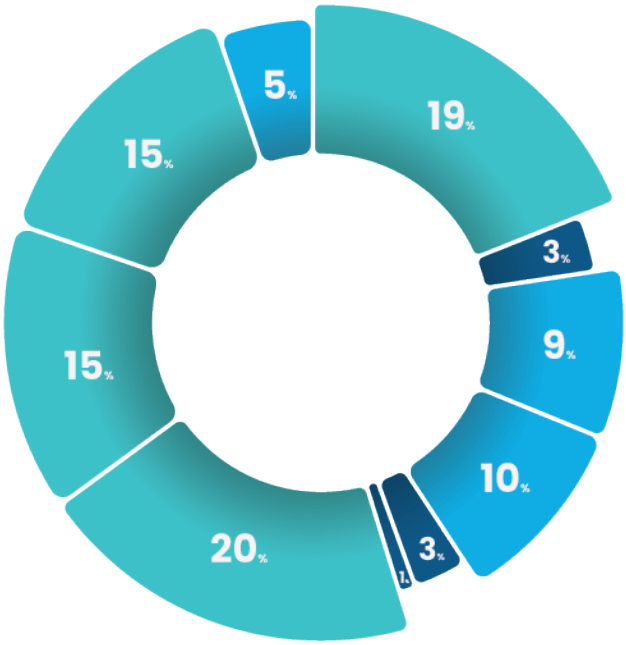
CYVO Wallet Development Timeline

3. TOKENOMICS

Token Symbol: CYVO

Token Type: Ethereum Multichain

Maximum supply: 1.5 billion



19%	Private Sale
3%	Public Sales
9%	Exchange Listing
10%	Staking
3%	Marketing Airdrops & Referrals
1%	Product Bounty
20%	Treasury
15%	Product Development R & D
15%	Founders & Management Team
5%	Advisory Panel

Useful Links

- www.cyvo.io
- www.linkedin.com/company/cyvo
- www.twitter.com/CYVOio
- www.instagram.com/cyvo.io/

Coming Soon

Facebook Medium Telegram