# NV Whitepaper

## NatiVault Hardware Wallet (NV)

Powered By

BC 5.0

7TH DEC, 2021

NatiVault LTD
50 Welton Rise, St. Leonard's-On-Sea, UK

# CONTENTS

# DISCLAIMER

*"The goal of this whitepaper is to inform potential contributors about potential opportunities provided by the **NatiVault** hardware wallet (hereinafter referred to as **NV wallet or NV**). As a result, this whitepaper should not be interpreted as solicitation or offer to invest. It should be noted that this whitepaper is not legally binding and does not impose any legal responsibility on anybody.*

*This whitepaper is not a legal contract and serves to describe the product's development process. The introduction and implementation of NV are dependent on a number of variables, including but not limited to the expansion of the cryptocurrency market, the acceptance of blockchain technology, user participation, the tokenomics used, regulatory risk, and so on.*

*The NV team has compiled material in the whitepaper to raise awareness about a next-generation hardware wallet that heralds a new paradigm in cybersecurity, and it is not obliged to take any action. The content in this whitepaper is solely for the purpose of disseminating general information. As a result, NV makes no guarantees about the accuracy or completeness of this material.*

*Anyone considering purchasing an NV wallet should be aware that the NV business model, whitepaper, future documentation, or material facts contained herein may change or require modification in the future to comply with law or regulatory requirements imposed by relevant jurisdictions. In this case, buyers or anyone purchasing the NV wallet/ NV tokens acknowledge and understand that NatiVault or any of its affiliates will not be held accountable for any losses or damages caused directly or indirectly by such modifications.*

*The NV team has compiled information in the whitepaper to raise awareness of a next-generation hardware wallet that heralds a new paradigm in cybersecurity, but it is under no obligation to take any action. This whitepaper's material is primarily for the purpose of disseminating general information. As a result, NV makes no representations as to the accuracy or completeness of this content.*

*While much attention and effort has been put into producing this whitepaper in order to offer the information and facts mentioned/represented in the material. However, NatiVault offers no assurances as to the accuracy or validity of the information contained in the whitepaper.*

*By agreeing to read this whitepaper, you have confirmed that you have understood, acknowledged, and agreed with the section titled "Disclaimer."*

# EXECUTIVE SUMMARY

Hardware wallets are physical devices that hold cryptocurrency private keys offline in an encrypted device. Every day, billions of dollars in cryptocurrencies are transferred between wallets in cryptocurrency marketplaces.

As the crypto industry embraces innovation on an exponential basis, the market is primed to witness the launch of a next-generation, agile hardware wallet that delivers foolproof security with a transformational user experience.

NatiVault (NV) is the first device in a completely new class of computer-integrated AI-powered hardware wallets based on patent-pending Zero Vulnerability Computing (ZVC) technology. ZVC has received early endorsement from a coalition of 10 EU cybersecurity specialists, including three Cybersecurity Centres of Excellence and is now being validated by the world's leading research institute- IMEC in Belgium.

**As a game changer, ZVC envisions a world in which fool proof cyber security is not a luxury, but rather a standard component in every online computing device.**

The design of the NV hardware wallet system is built on two proprietary, innovative layers of security. Its compact, minimalistic form effortlessly blends into the computer's USB port, allowing it to remain permanently connected. The device's unique value proposition, security features, user experience and creative business model- are all aimed at achieving quick adoption across market segments.

In conclusion, ZVC creates a future-proof computing paradigm. The NV device powered by the ZVC technology is more than just a hardware wallet. It is pertinent to mention here that NV is visible to consumers and competitors, as the metaphorical 'tip of the ZVC iceberg,' whereas the enormous body of the iceberg is concealed from view. The great majority of the technology's capabilities have yet to be commercialised. When ZVC is integrated with mobile phone driven IOT devices and when deployed within microchips within computers and made available across computing environments, it has the potential to usher in an exciting new era in computing history!

# BACKGROUND

According to Cybersecurity Ventures Report, If it were measured as a country, then cybercrime —which is predicted to inflict damages totalling **$6 trillion USD** globally in 2021 — would be the world's third-largest economy after the U.S. and China. And as if this weren't enough, cybercrime is estimated to cost the world **$10 trillion USD** by 2025.

This represents the greatest erosion of economic wealth in history, risks the incentives for innovation and investment, is exponentially larger than the damage inflicted from all natural disasters in a year, and would be more profitable than the global trade of all major illegal drugs combined.

## CYBERSECURITY BREACHES

In Legacy cybersecurity systems all cybersecurity breaches result from following two paradigms:

- **Vulnerability-related computer hacks** taking advantage of the attack surface inherently present in all computers, causing vulnerabilities that malwares exploit;
- **PII (Personally Identifiable Info)-related computer hacks** resulting from ID/credentials/PII theft, e.g., brute-force, dictionary-attacks, etc.

Currently all the cybersecurity techniques are limited to strategies that reduce the attack surface, and encrypt data stored in online devices to counter these paradigms. When pitted against the consistently growing technological prowess of hackers, these approaches seem hopelessly inadequate. Perhaps this is why most cybersecurity experts now conclude that fool-proof cybersecurity is impossible.

On the other hand, the global crypto market was valued at $2.3 trillion in the third quarter of 2021 (Dec), according to CoinMarketCap. The total value of the cryptocurrency market has risen to $128 billion. All stable coins had a combined market volume of $100 billion. NFTs worth over $17 billion USD would have been sold by the end of 2021. Every day, billions of dollars in bitcoin are moved from one crypto wallet to another on the crypto market.

Satoshi Nakamoto invented the Bitcoin wallet when he launched Bitcoin in 2008, and there are currently many different types and sizes of wallets, each providing unique benefits to its crypto users. The adoption of cryptocurrency has also resulted in a rise in cybercrime. It is estimated that a new hack attack occurs every 39 seconds, and that roughly 360,000 new

malwares are created every day! However, this does not preclude the usage of cryptography. Crypto wallets have over 70 million wallet customers by the end of March 2021 and this number is expected to grow further as mobile accessibility improves rapidly, according to Statista.

Cryptocurrencies are paving the way for the adoption of blockchain technology across a wide variety of industries. **In our studies we observe crypto early adopters to be responsive to new advancements in the sector. They appear to constantly seek key attributes such as speed, security, value for money and above all, superior user experience.**

## THE PROBLEM

In today's shark-infested cyber-world, Bitcoin is the most often targeted asset class by hackers. Even though hardware wallets are thought to be very secure, new research from ethical hacking organizations indicates that no hardware wallet is impenetrable. Findings like these, which we explored in depth in our Medium post cast doubt on the validity of the hardware wallet industry's main firms' statements. WALLET.FAIL, a group of cybersecurity specialists who proved in several ways that no hardware wallet can avoid the threat of a motivated and technically proficient attacker, made some of the most stunning discoveries.

Wallet.Fail and other ethical hacking initiatives have undoubtedly increased user awareness and comprehension of bitcoin cybersecurity problems. They have also significantly improved cutting-edge development by encouraging the community to think outside the box. It has also provided a realistic evaluation of what to anticipate from a safe and strong hardware wallet to the development community and other crypto stakeholders. In the controlled environment of a research laboratory, reverse engineering can disassemble nearly any device, but how the device operates in real-world settings may be a different issue. When it comes to comparisons, apples to oranges are most likely.

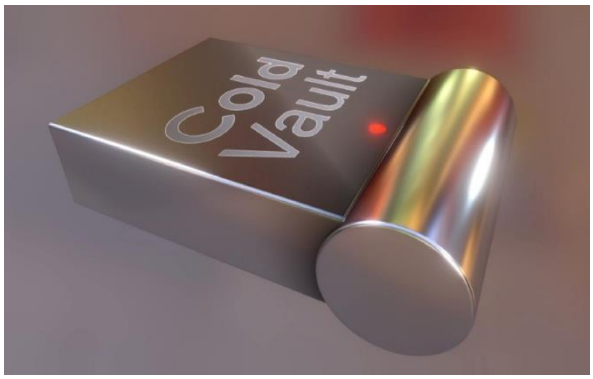
Nonetheless, the vulnerabilities highlighted by these hacking instances, as well as the security breaches published in many forums thus far, help us refine our approach to moving hardware wallet research beyond the bleeding edge. We focused on performance and usability concerns that hardware wallets may address to improve security, resilience, convenience, and value.

These aches and pains, as well as how they are treated, are divided into four groups:

### *1. Exploits in the Supply Chain:*

A "supply chain attack" is a devious and increasingly common kind of hacking in which an adversary inserts malicious code or even a hostile component into a trusted piece of software or hardware. A Chinese hacking group known as Barium carried out at least six supply chain attacks over the past five years. The costliest cyberattack in history was a supply chain hack that cost $10 billion to economies across Europe, Asia and America.

Most hardware wallets on the market allow an attacker to breach the device before it reaches the consumer. The WALLET.FAIL team demonstrated that an attacker with physical access to a Ledger hardware wallet may physically control the device while the user is unaware. An open-source hardware device design is available on GitHub for Ledger hacker's convenience.




### 2. Chip level attack / PCB-Level attack:

Reverse engineering, cloning, malicious insertion, side-channel assaults, and piracy can all occur on a chip/PCB. This option requires you to be physically close to the device. In the hands of an expert with the right tool, there is no product that cannot be reengineered and rendered vulnerable. The prior assumption, "All hardware wallets are hackable," is based on reverse engineering attempts to build chip level attacks against hardware wallets, most notably Ledger and Trezor, the most popular and ostensibly most secure in the hardware wallet market.

In a world where vulnerabilities are discovered and exploited with 350,000 new malicious programs daily, fool proof security in every conceivable scenario is impossible. Especially when a gadget is reverse engineered to allow entry. Hardware wallets are not meant to fall into the hands of an adversary, which may not be the case with any other device.

### 3. Firmware Attacks:

Physical access may or may not be required for firmware assaults. Despite this, nearly all ethical hacking tales involving hardware wallet firmware used physical access to effectively attack the Ledger and Trezor firmware. As previously stated, proximity reengineering attacks on firmware can only be countered by destroying the device and replacing it with a new one.

### 4. Server-End Attacks:

Ledger's database was compromised last year, resulting in hackers releasing the names, postal addresses, and phone numbers of 272,000 clients online. The hackers obtained access to the information by breaching Ledger's databases, and the stolen material was uploaded to Raidforums, a website for discussing compromised databases. While, the hack did not cause any asset losses to the Ledger customers, but it did make them victims of targeted spamming from marketers, spammers and fraudsters.

NV hardware wallet ecosystem tackles this pain point by staying in full compliance with GDPR. The users' asset always remains on the blockchain and their private keys and seed phrases locally encrypted in their devices. Moreover, any personally identifiable information (PII) required for customer registration is moved offline as soon as user registration is accomplished.

# THE SOLUTION

## BACKGROUND

After more than seven years on the market, the cryptocurrency industry's hardware wallet category is well-established and ready to scale up its appeal to the next level.

**We believe that the next generation of hardware wallets will need to deliver a next-generation user experience and value while also enhancing security.**

The solution design should be inspired by lessons gained from vulnerabilities in existing hardware wallets as well as being innovative in terms of furthering the state-of-the-art in cybersecurity.

The truth is that hardware wallets do nothing more than securely store the seed phrase associated with a specific wallet address, just the same as writing a seed phrase on paper and storing in a secure vault. This, then, begs the question: is a seed phrase printed on paper and stored in a vault more secure than a hardware wallet? The response is an obvious "NO".

So, what sets hardware wallets apart from the competition? Besides SECURITY, it all comes down to USER EXPERIENCE.

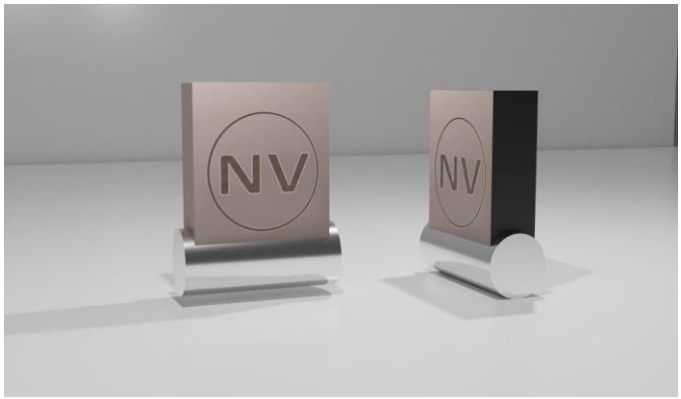
As a result, we focused our efforts on two critical areas in order to take the hardware wallet to the next level:

1. How could we provide superior value along with improved security and functionality over existing solutions?
2. How could we significantly improve USER EXPERIENCE?

**NatiVault** was our answer.

## NATIVAULT

*"A SOLUTION ROOTED IN DESIGN AND DEVELOPED WITH FORESIGHT"*




*"The way we approach design is by trying to achieve the most with the very least. Because as human beings, we understand clarity."* **Jonathan Ive, Designer, Apple**

" *If I'd have asked my customers what they wanted, they would have told me "A faster horse"* **Henry FORD, designer of Ford T**

Since 2007, our R&D team have put themselves in the shoes of our clients, imagining an entire wish list before users had even thought about it. We knew even back then that cybersecurity would only get more perplexing, difficult, and impossible to manage with the passage of time. And legacy thinking was to blame. NV is the culmination of over a decade's research. It offers a radical solution that is beyond easy comprehension of even cybersecurity experts...unless an effort is made to lift the veil of traditional thinking.

NatiVault introduces a totally new paradigm in cybersecurity, convenience, and value to the cryptocurrency business by providing and securing the hardware wallet where it belongs, where it should be NATIVE—the computer itself that conducts cryptocurrency transactions.

In comparison to a typical hardware wallet, the likelihood of your laptop or desktop being lost or stolen is practically none. Furthermore, because a gadget is frequently moved, it is more likely to be damaged, lost, or stolen. If your NatiVault hardware wallet is permanently incorporated into your PC, there is no general danger of theft or loss. Moreover, the device is designed in such a way that it ceases to operate if detached from the parent host system. This appears to be impossible on the surface since any data kept on a linked system cannot be deemed safe because it is subject to network failures. In legacy systems, keeping the hardware wallet connected to the computer 24/7 would be detrimental, as this would negate the objective of the hardware wallet, which is to keep the private keys offline.

The NV hardware wallet's technological achievement, on the other hand, is built on a fundamentally new cybersecurity paradigm: Zero Vulnerability Computing (ZVC) that not only renders it to be connected to the host PC 24*7 but at the same time offers a unique facility to store your crypto assets securely in an online computer.

# THE TECHNOLOGY

## ZVC (ZERO VULNERABILITY COMPUTING): INTRODUCTION

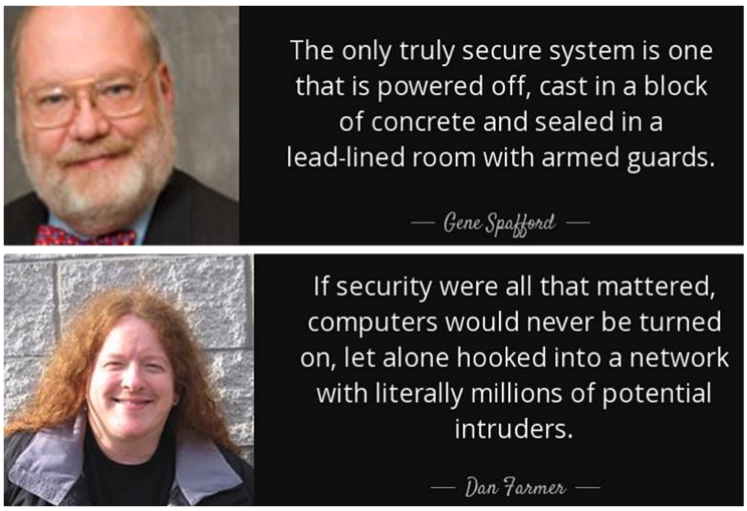
In Legacy cybersecurity systems all cybersecurity breaches result from following two paradigms:

- **Vulnerability-related computer hacks** taking advantage of the attack surface inherently present in all computers: the surface where computer's operating systems meet 3rd party applications, causing vulnerabilities that malwares exploit.
- **PII (Personally Identifiable Info)- related computer hacks** resulting from ID/credentials/PII theft, e.g., brute-force, dictionary-attacks, etc.

To confront these paradigms, legacy cybersecurity approaches are restricted to measures that decrease the attack surface and encrypt data stored in internet devices. Because these techniques fall short of perfection, cybersecurity experts conclude that fool-proof cybersecurity is unattainable.

Any data stored in a networked computing device is considered at risk in prior art.

***"This is a world in which the promise of secure digital technology turns out to be in many respects a poisoned chalice.***" – CLTC, Berkley"




Zero Vulnerability Computing (ZVC) challenges such assumptions with a vision of a fundamentally safe system that does not need to be turned off, cast in concrete, or locked in a lead-lined chamber to be secure and immune to hack attempts. **Maintaining a computer online while keeping the stored personally identifiable information (PII) safe is a prior art impossibility that ZVC challenges**.

## NATIVAULT: WORLD'S FIRST ZVC POWERED HARDWARE DEVICE

The NV hardware wallet is the first device to incorporate an innovative new DESIGN in disrupting the cybersecurity status quo, deploying the following two-pronged approach:

1. Creating an in-computer offline storage (**ICOS**) within a network-connected device (US Patent Application 63/228,122, August 1, 2021).
2. Completely obliterating the attack surface present on a computing device deploying a Supra OS (**SOS**) software (US patent Application 63/202,188, May 31, 2021).

## HACKERS' DOUBLE JEOPARDY WITH ZVC

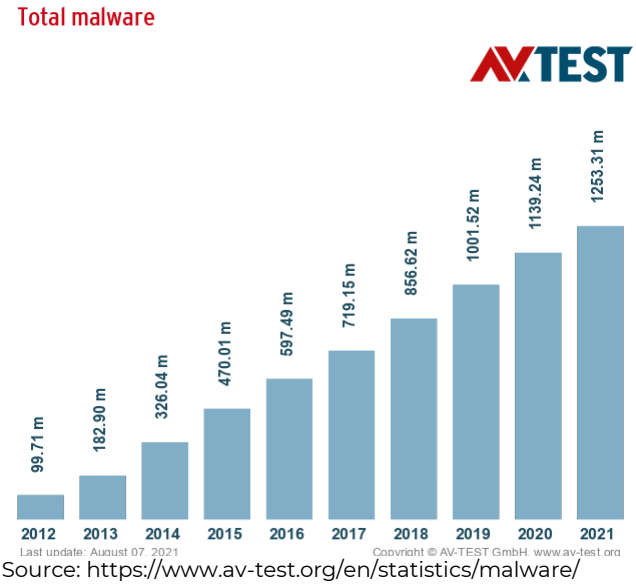
ZVC's two fundamentally novel design elements (ICOS and SOS) deal a double strike that leaves no maneuvering space for hackers.

The combination of SOS and ICOS frustrates the attacker while simultaneously making the NV device cyber safe and offering the device owner with unprecedented ease. The terms ICOS and SOS are discussed in further detail below.

### *Supra-OS (SOS) Obliterates a computer's attack surface*

**Background:** An attack surface is essentially the entire external-facing area of a computing environment. It contains all of the vulnerabilities or attack vectors a hacker could use to gain access to a computing system. The magnitude of the attack surface is directly proportional to the density of vulnerabilities.

With the advent of IoT and proliferation of connected devices, attack surface and consequently vulnerabilities have exponentially grown. Every day, the AV-TEST Institute registers over 350,000 new malicious programs (malware) and potentially unwanted applications (PUA). Over the past decade malware has grown from about 100 million in 2012 to 1.3 billion in 2021. This growth in vulnerabilities and proliferation of attack surface is essentially attributed to a very common practice of Code reuse in software development due to its various benefits. Use of both commercial and




Source: https://www.av-test.org/en/statistics/malware/

open-source components in development increases vulnerabilities. However, such a practice causes large-scale security issues since one vulnerability may appear in much different software due to cloned code fragments.[1] The rising trend has become a major reason for the constantly expanding attack surface in the past decade. Zhang et al[2] recently demonstrated that many seemingly unrelated software apps share a significant common attack surface. On top of the software development trends that increase the attack surface, the time frame of vulnerability exploitation has compressed by 93%. Now it is only 3 days before a vulnerability is exploited, against 45 days in 2006.[3] Recent report from Cyber Security Ventures predict zero-day cyber-attacks to rise from one per week to one per day.

Though not as extensive as the traditional computing system, legacy hardware wallet devices also come with inherent attack surface, the sources of which are the following:

- **Multiple hardware components** (e.g., STM32, ST31 chips, PCB, etc.): Each hardware component has its own attack surface. As explained subsequently, this attack surface is because of the permissions it grants to the firmware for running applications. The more hardware components, the higher will be the attack surface.
- **Firmware:** The firmware that hardware wallets deploy may leave vulnerabilities, which if not patched reveal the attack surface.
- **Application Layer**: The application layer sitting on the firmware may present secondary attack surface that hackers can use to exploit.

**Current measures against the attack surface:** In the current state-of the-art, the approach to improving the security of a computer system is to measure the attack surface of a computing environment the system is exposed to, and minimize it with the following basic strategies:

i) reducing the amount of code running,

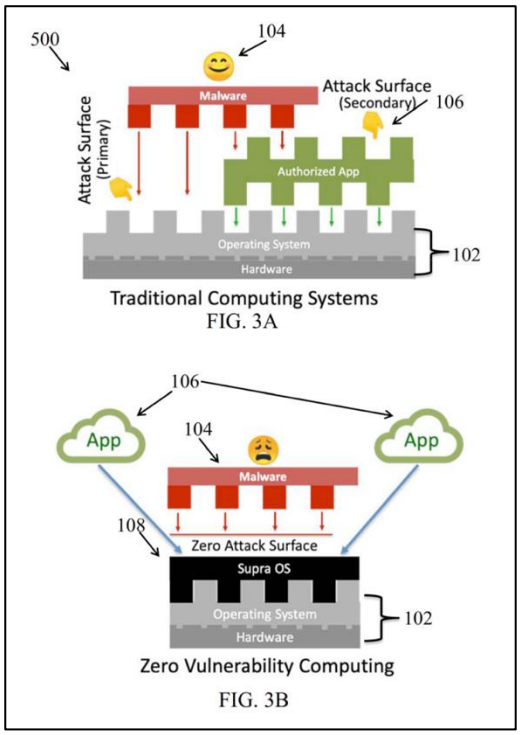
ii) reducing entry points available to untrusted users, and,

iii) eliminating services requested by relatively few users.

The Zero Trust architecture by NIST also suggests a similar strategy. Legacy hardware wallet devices also encounter the problem by releasing patches for the vulnerabilities. Although the attack surface reduction helps prevent many security failures, it does not mitigate the damage an attacker could inflict once a software vulnerability is found.

[1] Stellios, P. Kotzanikolaou, C. Grigoriadis, "Assessing IoT Enabled Cyber-Physical Attack Paths Against Critical Systems", Computers & Security, 2021, 102316, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2021.102316.
[2] Zhang M., et al. (2019) CASFinder: Detecting Common Attack Surface. In: Foley S. (eds) Data and Applications Security and Privacy XXXIII. DBSec 2019.
[3] https://solutionsreview.com/cloud-platforms/sonatype-state-of-software-supply-chain-report/

**How SOS works**: Generally, all computer devices must give rights to third-party apps. Without these rights, computers are worthless. While legitimate programs use these rights to enable computers to do amazing feats, bad actors frequently abuse the permissions to create an attack surface and vulnerabilities. Hackers use these flaws to infiltrate the machine and install malware remotely.




To accomplish ZVC, NV hardware wallet employs a two-pronged strategy: first, keep the attack surface low with a minimalistic design, and second, apply Supra OS (SOS) software. SOS was created to eliminate computer vulnerabilities by fully obliterating the attack surface of a computing device, which bad actors frequently exploit to insert malware. (May 31, 2021, US patent application 63/202,188). Please see the following illustration, which has been derived from the SOS patent application. SOS implementation in NV hardware wallets is less complicated than on standard computer systems.

Because the NV hardware wallet is a single-purpose device, the SOS script is built to reject all third-party permissions while enabling its native wallet applications to function.

### *In -Computer Offline Storage (ICOS) secures in-computer personal data from network attacks:*

Over 25 billion linked gadgets remain susceptible in today's ever-expanding Internet.

According to cybersecurity experts, data within a connected device can never be completely safeguarded since network exposure is always risky.

No data is safe unless you are offline. However, data accessibility is substantially hampered while we are away, prompting us to wonder and ask: ***Why don't computers have built-in offline storage?***

Our response is ICOS - world's first in-computer offline storage (**ICOS**) device with a simple user-controlled instant OFF/ON toggle switch for secure data management. A thematic representation may be found here: https://skfb.ly/☹ootNO

All in-computer data storage must remain online if the computer is linked with today's technology. There is no way for a networked device to make the saved data safe while being connected to the online network. As a result, perfect cybersecurity for computer equipment is seen as unattainable. ZVC overcomes this impossibility by developing a hardware wallet that can be permanently installed on any connected computer while always remaining offline and easily accessible using a toggle switch.

Our novel design marks a fundamental paradigm shift in the hardware design of future computing devices, providing in-computer offline storage (ICOS) technology for the first time in computer history, shielding data from the risks of network vulnerabilities. This revolutionary hardware design for in-computer offline storage (ICOS) is patent pending (US Patent Application 63/228,122, August 1, 2021) and is utilized in the development of the NV hardware wallet (See illustration 110).

The Offline/Online status of the NV device is controlled by the device's owner through an ON/OFF toggle switch (116), which the data owner may deploy to keep the data offline or quickly connect it to the host computer at the data owner's request. As a result, the NV hardware wallet provides a secure offline storage space directly in your connected computer to preserve the seed phrase and private keys while also making them instantly available for processing when needed.

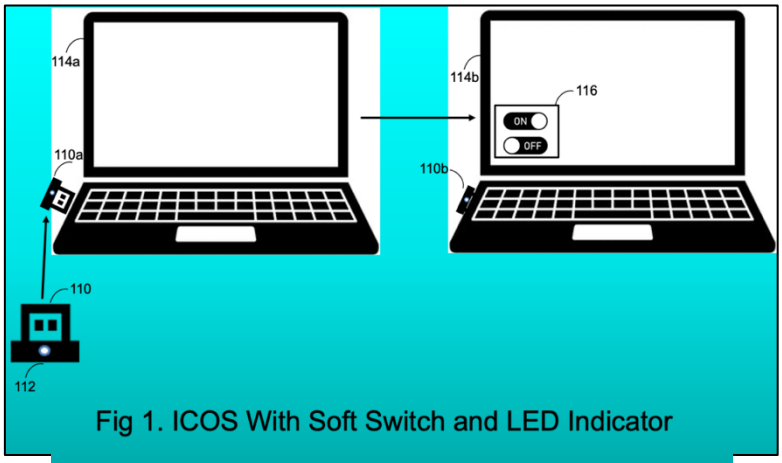



Fig 1. ICOS With Soft Switch and LED Indicator

Source: (US Patent Application 63/228,122, August 1, 2021

**Moreover, future iterations of NV hardware wallet would incorporate encryption technologies like Partial Homomorphic Encryption (PHE) to keep the data in an encrypted state even when it is in computational state, ensuring the data security throughout the entire cycle of Storage, Processing and back to Storage.**

**ZVC in a nutshell:** In legacy computers, neither the attack surface is completely eliminated, nor the device can store data offline when connected to the online system, making foolproof cybersecurity impossible. ZVC utilizes two novel design elements, ICOS and SOS, which deal a double strike to hackers to render NV devices cyber secure.

ZVC has accumulated significant momentum and support with the collaboration of at least ten European Universities and Research Institutions (including three Cybersecurity Centres of Excellence), as well as funding from the European Commission to test and validate ZVC at Europe's top Belgium based research organization- IMEC.


Even though ZVC has the potential to significantly impact the $6 Trillion cybercrime space and transform the way people use the Internet and process data towards a safer and more resilient cyberspace, our present focus is to take baby steps before taking on mammoth initiatives. Riding on a secure, simple, and user-friendly NV hardware wallet- low profile entry into the market- seems a good strategy to embark on.

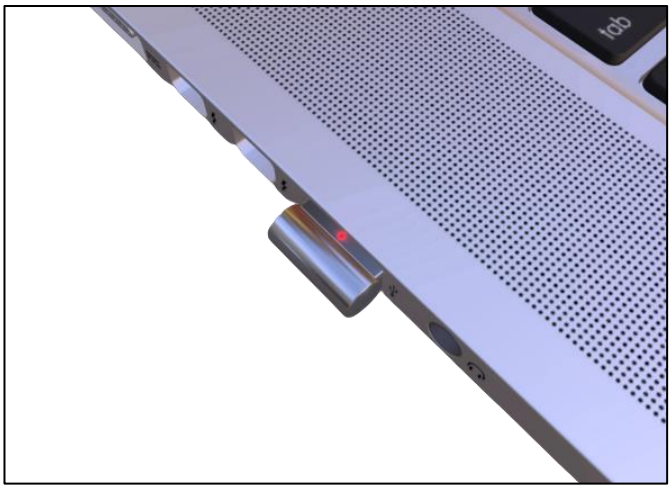
## WHAT IS NATIVAULT (NV)?

NatiVault is a fresh, new, and original inception in the market of crypto wallets backed by the patent pending technology ZVC. NV is the First device in a whole new class of computer-integrated hardware wallets that combine next-gen security with previously unheard-of superior user experience.

## FORESIGHT

- NV is the first hardware wallet that stays integrated to your PC 24/7, in a most secured environment.
- NV is world's first hardware wallet that integrates AI enabled SSID module (with Face Recognition and Password combination in an encrypted form) for signup, login and singing-in of wallet transactions.
- Additional security by linking wallet seed phrase with SSID Module, making it the first hardware wallet in the world that doesn't force its users to save seed phrase on a piece of paper for wallet recovery.
- Seed phrase stored in a binary encrypted form that can only be accessed with user SSID, making it virtually impossible to hack even if the device is stolen or lost.
- Offers to store wallet seed phrase on an offline server that can only be prompted online with user SSID.
- Anti-theft/ Anti-custody protection that disables the device automatically when stolen, lost, or unmounted from the host computer.
- Each device is identified by a unique ID, giving it exclusivity, allowing it to be readily traced.
- NatiVault is the world's first hardware wallet backed by the NV utility token.

- The device runs on an in-built application that ceases to operate if it is interacted by any other software.
- If any concurrently running software or process attempts to perform any action over the connected device, the device instantly goes offline, rendering your crypto assets secure.
- Works with Linux, Mac, Android, and Windows platforms (current prototype is a Linux version and other versions are in development).
- Supports ERC20, BTC and multiple hot blockchains.




- The NV hardware wallet ecosystem is entirely GDPR compliant. Users' assets are always stored on the blockchain, and their private keys and seed phrases are encrypted on their devices. Furthermore, after completing user registration, all personally identifiable information (PII) required for client registration is moved offline.

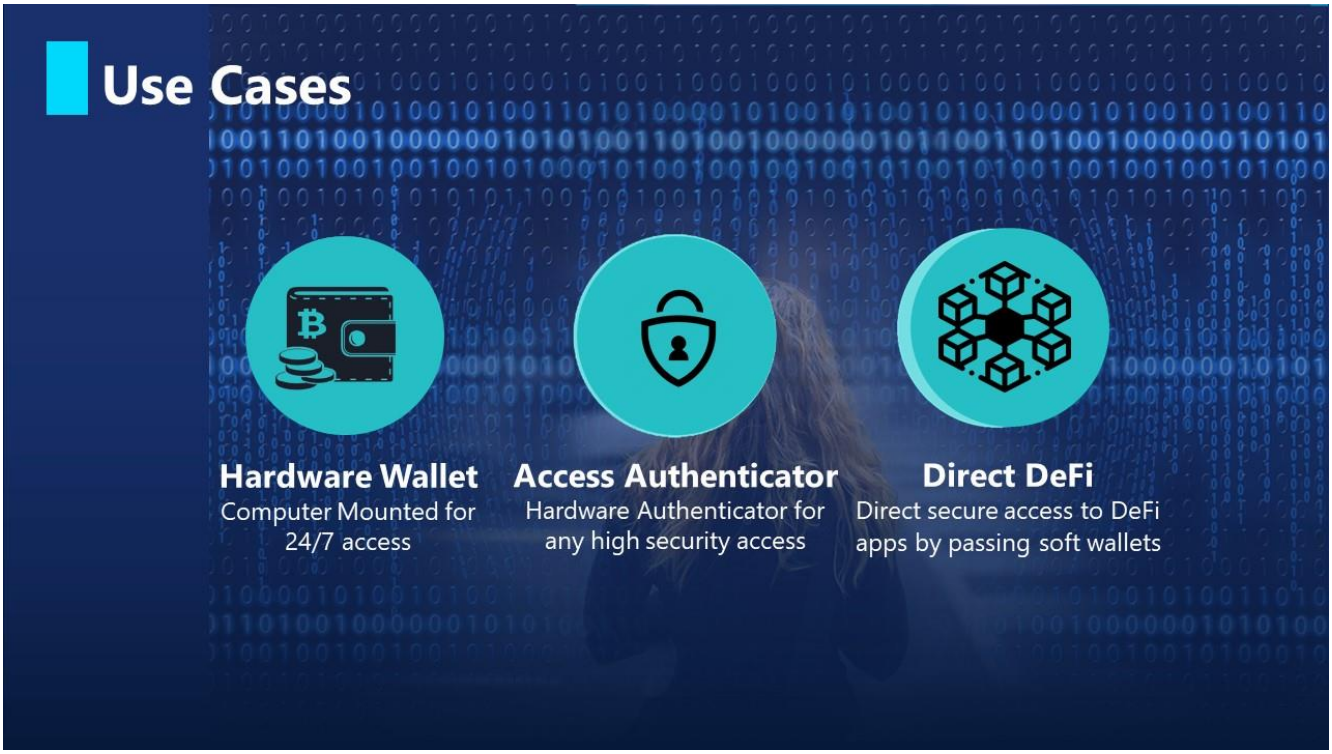
Aside from the capabilities listed above, the NV hardware wallet has the following advantages over competition:

- Easy to use UI- user interface allows holding multiple cryptocurrencies
- Automated
- Superior Functionality
- Secure
- Always connected to the host computer
- Affordable @ Just US$ 50 Vs advanced versions of competitor wallets priced 2 or 3 times the price of NV

## NV: OFFERING MULTIPLE SERVICES WITH A SINGLE HARDWARE

Although NV is designed to work as a hardware wallet, its 24/7 connectivity and compact design is based on NAND flash memory chips without the need of secure microcontroller chips like STM32. Such attributes extend its utilization beyond just hardware wallets.

In addition to being a 'future-ready' hardware wallet, NV also fits into the rapidly growing market of hardware authenticators on the lines of an authentication hardware device to sign in to various online or offline platforms. Additionally, NV would provide direct access to DeFi markets, bypassing soft wallets.




## ADDITIONAL SECURITY FEATURES BUILT INTO NATIVAULT

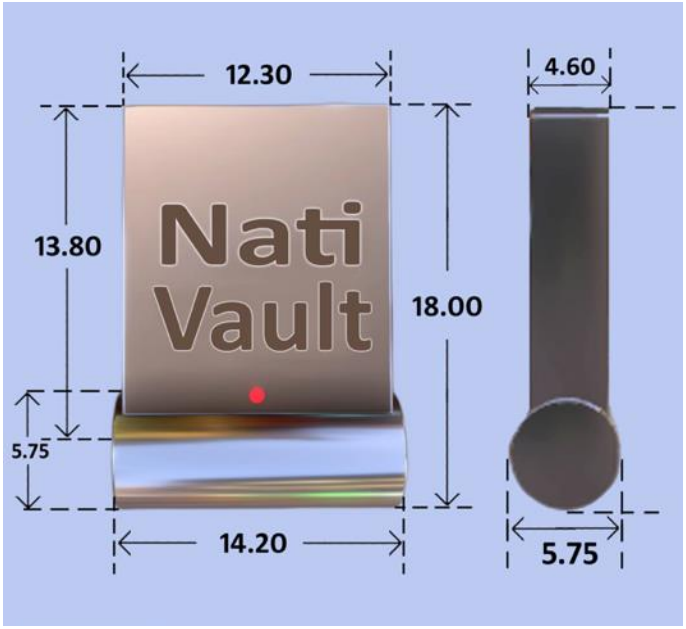
In addition to the novel cybersecurity features provided by Zero Vulnerability Computing, NV incorporates next generation security features provided by state-of-the-art hardware wallets on the market:

- **2-Factor authentication:** To complete a transaction, an OTP/Google authenticator code is generated and should be submitted before the time limit expires.
- **Data encryption:** Using cryptographic characteristics, data encryption ensures super-secure data and information protection.
- **Jail login:** When NatiVault detects invalid credentials, it would instantly deactivate the device.
- **Anti-denial of service (DOS):** It protects the wallet from large requests that are concomitantly sent to the wallet when it is connected to the internet.
- **Anti-distributed denial of service (DDoS):** When linked to the internet, it protects the wallet against surging traffic generated by multiple sources.
- **Server-side request forgery (SSRF):** It protects the wallet from several vulnerabilities that might attack the wallet when it is connected to the internet.

# TECHNICAL SPECIFICATIONS

NV's small form factor, compact, solid-state device is compatible with USB TYPE A and TYPE C ports. The NV hardware wallet's simple design with zero detachable parts makes it very durable and nearly impossible to hack.

The small design practically blends into the curves of the host computer, allowing it to be installed 24 hours a day, seven days a week, keeping your assets offline yet instantly accessible whenever needed.




The following are the technical specifications in detail:

- **Single mold metal device** guarantees that the device is handed to you without any other hardware accessory being installed, which might interfere with the hardware wallet's secure operation. The hardware body is made of a single piece of Zinc Alloy metal which allows for a compact form while still providing a robust glossy appearance and essential durability against wear and tear.
- **Tiny Design:** Dimensions of NatiVault's current version are displayed in the image above.
- **Compact NAND chipset:** A tiny NAND microchip encoded with SOS and ICOS codes is housed within the hardware enclosure. SOS completely obliterates the device's attack surface, whereas ICOS maintains the data offline, except when processing, rendering the device malware proof while providing a safe offline storage space on the online PC. Once the device is sealed, the NAND chipset is designed to prevent any additional third-party software installation, thereby making any PCB level or Firmware assaults next to impossible.
- **Light Weight:** NatiVault weighs as little as 5 grams, making it a perfect accessory that can be left mounted on your host PC 24/7.

# COMPETITIVE ADVANTAGES

| | LEDGER | SATOSHI LABS | ELLIPAL | NATIVAULT |
|---|---|---|---|---|
| PLATFORM | Window, Linux, Mac, Android, Chrome OS | Windows, Linux, Mac, Android | Android, iOS | Windows, Linux, Mac, Android |
| **CUSTOMER EXPERIENCE** | ** | ** | * | ***** |
| **2-LAYER PROTECTION** | **No** | **No** | **No** | **Yes** |
| OPEN SOURCE | No | Yes | No | Yes (hybrid) |
| **WEIGHT** | **34 gms** | **16 gms** | **138 gms** | **5 gms** |
| INTERFACE | BLE, USB-C | MicroSD, USB-C | Camera | USB Type C & A |
| SIZE | 72x19x12mm | 64x39x10 mm | 119.4x64x9.9mm | 18x5x4 mm |
| **PLUGGED- IN CONVENIENCE** | **No** | **No** | **No** | **Permanent** |
| **FACE RECOGNITION** | **No** | **No** | **No** | **Yes** |
| **BIOMETRIC AUTHENTICATION** | **No** | **No** | **No** | **Yes** |
| **ANTI THEFT PROTECTION** | **No** | **No** | **No** | **Yes** |
| COST | >$50 | >$50 | >$50 | =$50 |
| VALUE GRAB OPPORTUNITIES | No | No | No | Yes |
| **HARDWARE-AS-A-SERVICE MODEL** | **No** | **No** | **No** | **Yes** |
| PRODUCT LINE EXTENSION | No | No | No | Yes |
| **NFT** | **No** | **No** | **No** | **Yes** |
| **BACKED BY UTILITY TOKEN** | **No** | **No** | **No** | **Yes** |

## NV: COMPETITIVE FROM THE START!


## WORKING OF NATIVAULT

1. Plug the gadget into the PC's USB port.
2. The device resident software automatically identifies the system OS and installs the required utilities.
3. Configure Face Recognition and Password to generate the device's unique ID.
4. The encrypted user ID is saved to the device and matched on each log in / transaction activity, assuring the security of crypto assets.
5. You have an additional option to store your seed phrase on an offline server for wallet recovery using the set SSID.
6. Inbuilt UI that can be launched with just 1 click, bringing your crypto assets online
7. The device instantly launches an in-built application instance, providing the option of connecting your NatiVault to the host PC or to keep it offline.
8. SOS software runs a program to ensure that no other third-party software is operating while you transact your crypto holdings.

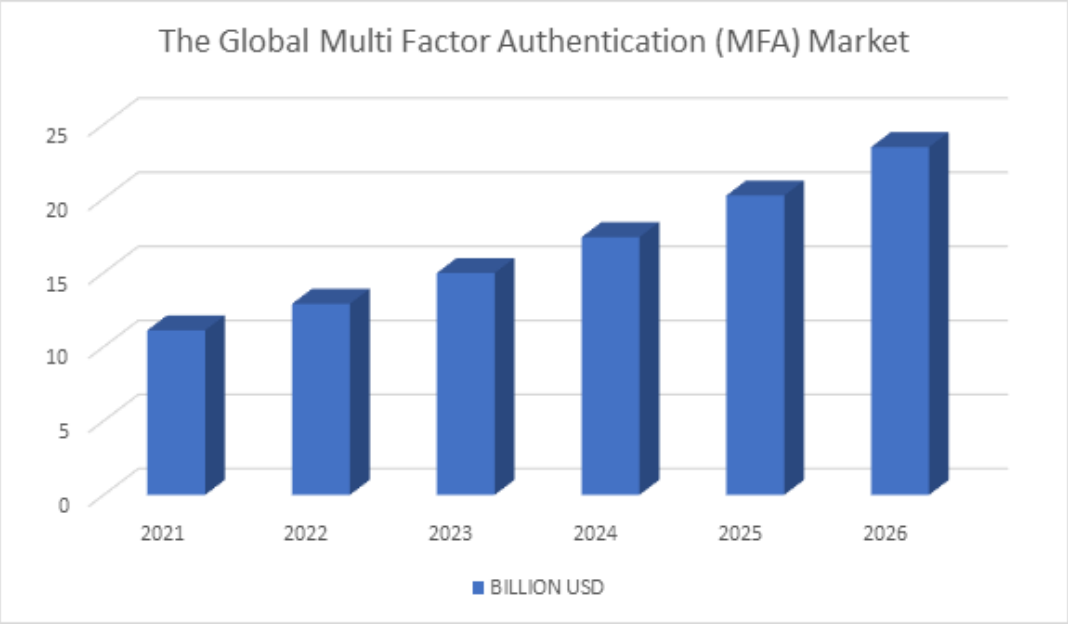
9. If the device is tampered with by other programs, it instantly ejects itself from the host PC, prohibiting any unwanted infiltration.
10. The NatiVault ecosystem does not interact with the system unless it is prompted ON (online) again, thus there is no need to remove it from the PC.

- Artificial Intelligence allows easy and secure log-in due to the AI-enabled face recognition module.
- Easy to use user interface allows transacting with confidence.
- Using AI methodology and encryption techniques, the private keys and seed phrase are maintained locally in the device- secured and encrypted.

## NV MARKET

The global Multi Factor Authentication (MFA) market size is projected to grow from USD 11.1 billion in 2021 to USD 23.5 billion by 2026, at a Compound Annual Growth Rate (CAGR) of 16.2% during the forecasted period[1]. An exponential rise in security breaches, fraud, data identity thefts, surge in use of BYOD/ IoT devices, high demand for cloud-based MFA solutions and services, high volume of online transactions, and stringent government regulations are some of the driving forces for the phenomenal growth of this market.

Apart from granting access to the secure systems, MFA is used to secure transactions and protect customers from phishing attacks and fraudulent transactions. Integration of such systems by healthcare, retail, and BFSI sectors, offers an immense opportunity for the growth of MFA authentication.




https://www.marketsandmarkets.com/Market-Reports/multifactor-authentication-market-231220047.html

[1] https://www.marketsandmarkets.com/Market-Reports/multifactor-authentication-market-231220047.html

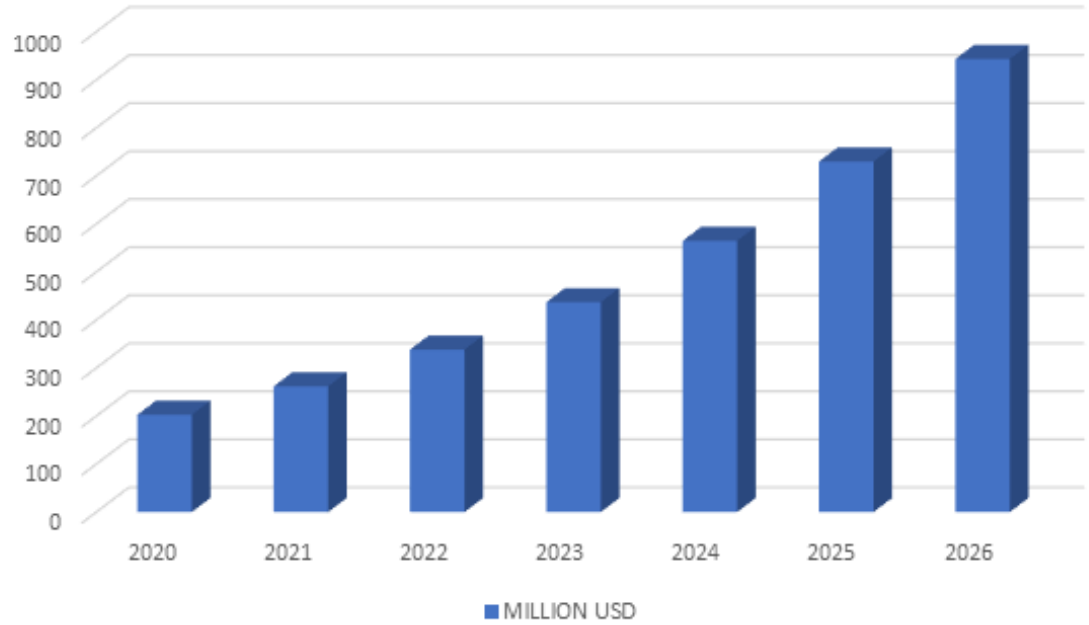
## NV INITIAL TARGET MARKET

NV hardware, owing to its multifunctionality can be considered as a prominent technology that can dominate both the hardware wallet as well as authenticator segment right from the start. For positioning NV hardware device in the market, we have classified 2 niche segments that can certainly be considered as initial serviceable market for NV, while the total addressable market remains the Multi factor Authentication Market.

### Hardware Wallet Market

> *"The hardware wallet industry was valued at more than $202.4 million in 2020, and it is anticipated to reach $878 million by 2026. In this fast-developing sector, over a dozen hardware wallets vie for market share."*

EXPONENTIAL RISE IN THE CRYPTO CURRENCY HARDWARE WALLET MARKET




https://www.mordorintelligence.com/industry-reports/hardware-wallet-market

Base year: 2020. **CAGR: 29.24%**

Along with its use as a hardware wallet, NV is also designed to integrate the Hardware Authenticator functionality.

### Hardware Authenticator Market

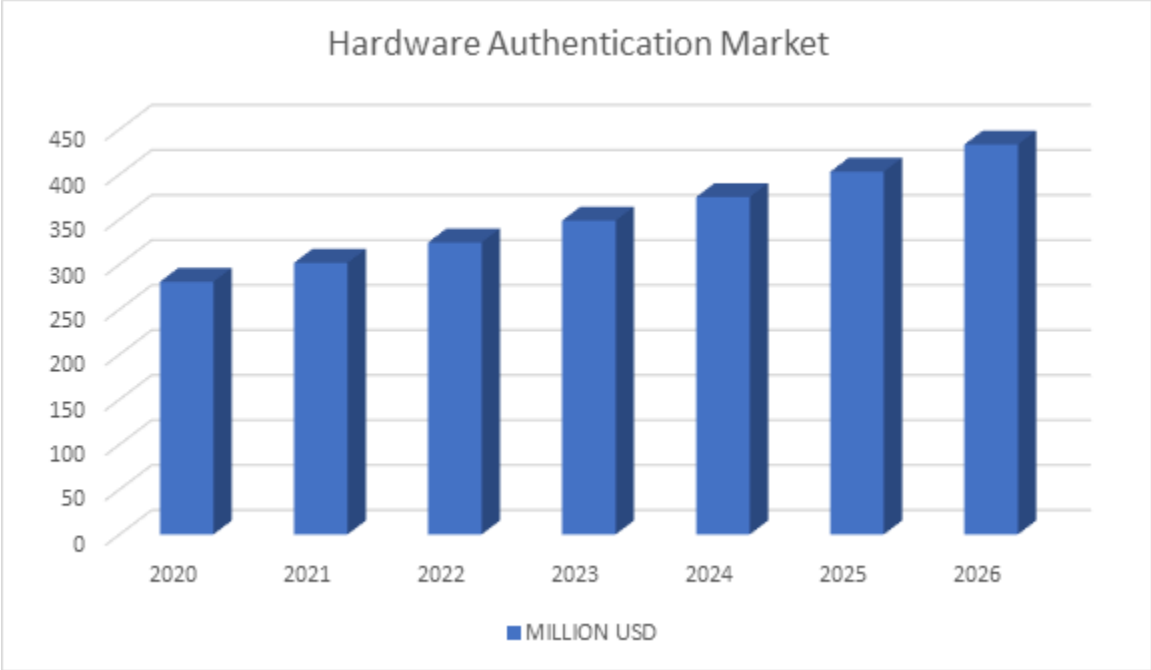
Although the MFA ecosystem involves many components based on Hardware, Software Solutions, and Services, the Hardware authentication is gaining wide acceleration owing to its easy adaptability and wider appeal. Hardware authentication is an approach that

relies on a dedicated physical device (such as a **token**) held by an authorized user, in addition to a basic password, to grant access to computer resources.

The market is still in its early stage of adoption with new technologies and players arriving. Currently, the market only has a few players offering different product types (USB Tokens, SIM Tokens, Mini Tokens) in Connected, Disconnected and Contactless variants. A prominent player is Yubico, which adopts the FIDO U2F authentication standard, and is popular with the presence of several models. Google also sells its own key, called the Titan, which includes a spare key with Bluetooth functionality. Other security key manufacturers include Kensington and Thetis.

NV technology can potentially cater to a wide market segment even if one takes the conservative approach of considering only the HARDWARE OTP TOKEN AUTHENTICATION MARKET as another niche market for NV.

> *"Hardware OTP Token Authentication Market was valued at USD 280.6 million in 2020, and is expected to reach USD 433.1 million by 2026, at a CAGR of 7.5% over the forecast period (2021-2026)[1]."*

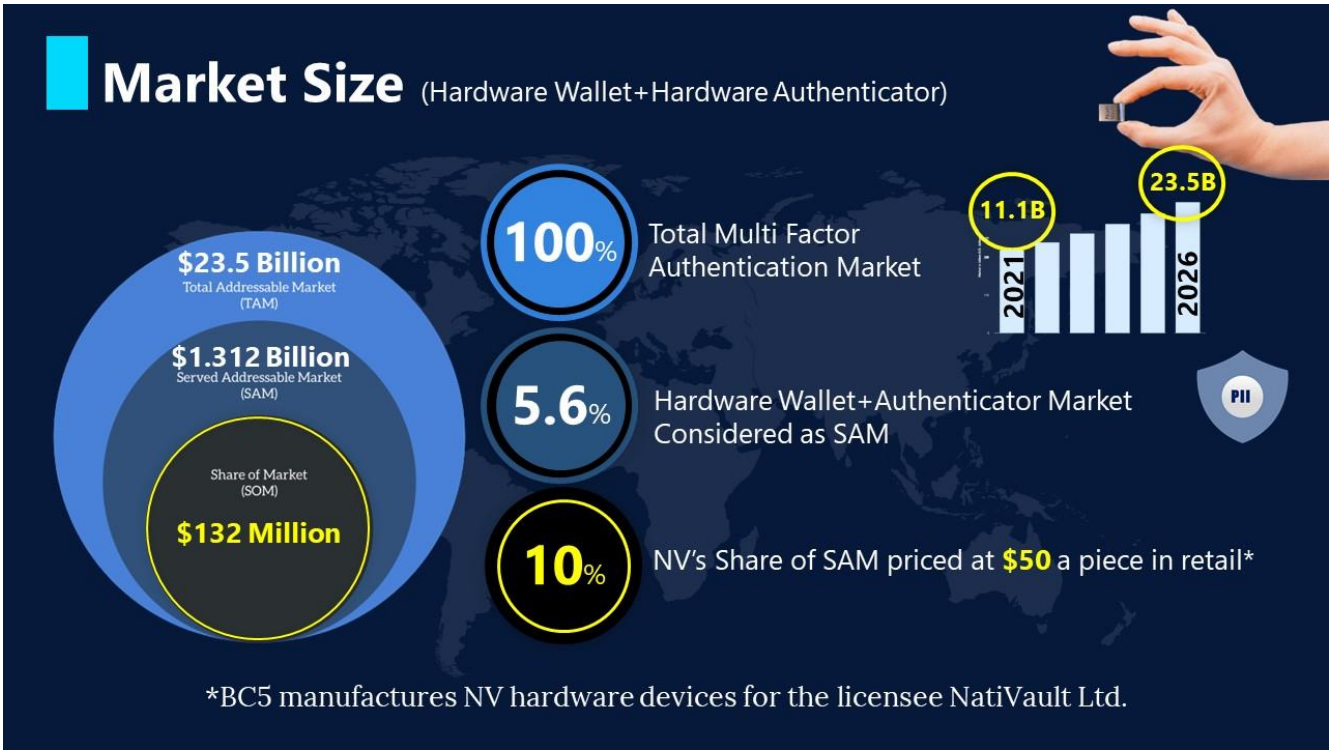



https://www.mordorintelligence.com/industry-reports/hardware-otp-token-authentication

Base year: 2020. **CAGR: 7.5%**

## MARKET PROJECTIONS

Owing to the multifunctional nature of NV hardware, company intends to project NV hardware not only for the crypto market but also for the hardware authentication market.

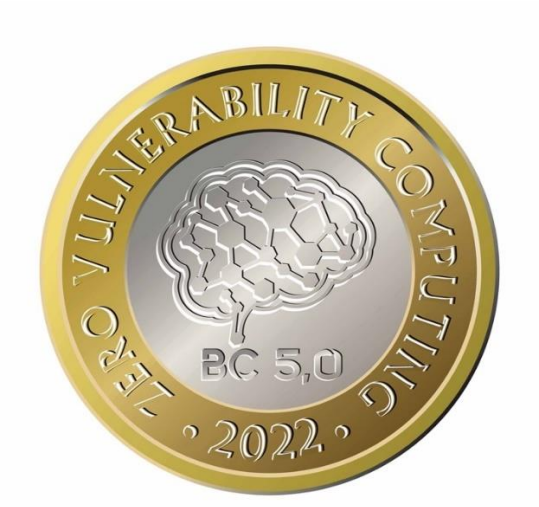



****Note: The market projection only includes the revenue generated out of hardware sales and does not factor NV tokenomics*

The Multi Factor Authentication (MFA) market can be considered as the total addressable market (TAM) for NV. The company intends to design NV as a hardware wallet as well as the authenticator device & hance the combined hardware wallet market and hardware authenticator market, forms the serviceable market for NV hardware device. With just 10% penetration in the combined serviceable markets, NV's market share will be worth no less than $132Mn in the coming 4 years.

These are a few possible outcomes that can arise in the different market positioning of NV devices tomorrow. When the NV market strategy projects NV technology, it does so in a realistic manner, securing investors' interest should things turn south tomorrow.


## THE NV TOKENOMICS & BUSINESS MODEL


### TOKEN DETAILS

Adhering to the ERC-20 token standards, NV tokens would function as ERC20 utility tokens. As a utility token, NV offers utility convenience within the DeFi space. At the same time, the product would be resilient, constantly growing and evolving in response to an evolving future with significant possibilities.

## TOKEN UTILITY

**DeFi Primitives:** Millions of small firms onboard various blockchain ecosystems almost every day. As a result, the world is witnessing an exponential rise in the DeFi space, and companies are scrambling to create value and be seen as relevant.

The NatiVault ecosystem leverages blockchain technology when providing its services.

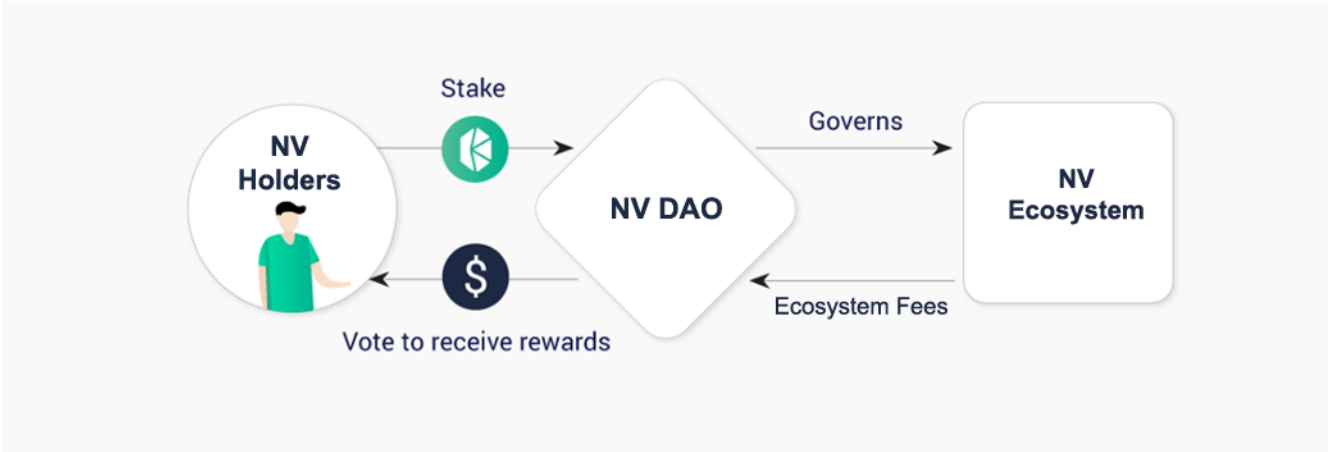
**A major feature in the utility value of NV is its opening of safe access to a wider DeFi ecosystem.** NV tokens will be used as the medium of exchange for trade protocols, lending/borrowing protocols, staking protocols, and a variety of other DeFi services across the Ethereum, Polygon, and other EVM compatible chains. The company aims to achieve this through its B2B association with diverse DeFi protocols and their exclusive integration with NV ecosystem.

The NV token model allows new entrants to navigate the DeFi space almost effortlessly. The following value-capture strategies are designed within the NV tokenomics:

**Staking:** This forms the backbone for sustained income for the NV DAO as well as the individual stakers. Rewards and perks are offered to individuals that stake their NV tokens, essentially pledging their tokens to the network. The network pays them with handsome rewards in NV tokens, effectively allowing stakers to earn profit and accessing value-added services.

**Governance:** The NV DAO facilitates decentralized governance. Stakeholder feedback offers participants an additional incentive to stake. This would qualify participants not just for rewards but would also determine the future course of action for the DAO. Besides governing rights, DAO membership would open access to exciting incentives such as airdrops, staking interests, and future investment opportunities arising through NV investment pool. In addition, **DAO members would automatically qualify to receive a 50% share of network fees of NV in proportion to their staked amounts.**

To participate in the NV DAO, one must stake at least 100,000 NV tokens.



For decentralized governance to be effective, incentive structures must accurately reflect both its positive and negative effects. In other words, governing authorities should be rewarded for good outcomes and penalized for poor ones. The NV ecosystem will aid in this endeavor in two ways:

NV DAO governance allows for direct involvement.

A stake utility offers financial incentives for participating in NV and enhancing its revenue generation. In addition, the governance utility provides participants with the means to enact these incentives.

In the NV environment, these two utilities will work together.

As a result, NV will have only one staking pool. With this pool, NV tokens will offer representation and stake incentives, while also providing insurance coverage where needed.

**Availing added NV Services:** For normal hardware wallet functionality, the NV ecosystem would not charge an upfront fee to users. Based on the platform usage, the token concept would incorporate a transaction fee for other added services. In addition to the rebated fees associated with DEX and DEFI, staking NV tokens gives token holders the opportunity to opt into future business opportunities that will add value and utility to the token.

**By including a buy back and burn mechanism once we reach specific income-generating milestones, scarcity and preservation of long-term value is created for NV tokens.**

NV burning model ensures burning of 50% of NV token received in ecosystem fees, throughout its life cycle and a periodic burn of 2% token every year out of the circulating supply.

The NV ecosystem plans to buy back NV tokens from the circulating supply with 20% business profit and then burning it.

This buy-back and burn mechanism would be executed till 40% of the total supply of NV tokens are burnt.

**The NV DeFi ecosystem would be accessible from the NV wallet after staking a mere 100 NV tokens.** A minimum of 1000 NV tokens would have to be staked to receive airdrop rewards.

## NFT OFFERING

Non-fungible tokens took the art world by storm earlier this year with a virtual artwork by Beeple selling for $69 million. This was followed by Jack Dorsey's auction of his first tweet for $2.9 million. NFTs are a type of digital asset that may be used to prove ownership of a one-of-a-kind virtual object such as online photographs and videos or even sports trading cards. Physical assets, which are becoming increasingly rare over time, are the next line of defense for NFTs. The NV hardware wallet has the potential to become one of the world's most distinctive collector treasures over time.

The underlying technology behind NatiVault, ZVC (Zero Vulnerability Computing), is a breakthrough technology with the potential to create a major milestone in the history of computers by rendering them un-hackable through two radical design attributes that first create offline storage within a connected device (ICOS) and second completely obliterate the attack surface that hackers exploit (SOS). NatiVault, the world's first ZVC-enabled device, clearly has the potential to be categorized as a rare collectible. Furthermore, the group intends to manufacture four ZVC-enabled NV (Platinum, Gold, Silver and Bronze) devices that will be auctioned off in a well-known NFT marketplace. NV aims to release 1554 devices in the following order of rarity.

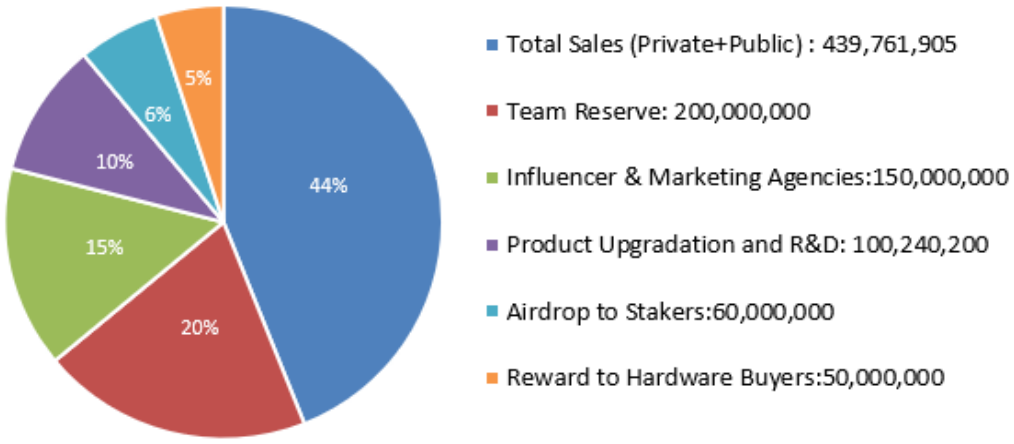
| Collectible | Quantity |
|---|---|
| NV Platinum | 6 |
| NV Gold | 36 |
| NV Silver | 216 |
| NV Bronze | 1296 |
| **TOTAL** | **1554** |

In addition to exploring the possibilities of NV as a collectible NFT, our business model will offer the world's first physical asset (NV device) tokenized as Non-Fungible Tokens- the NV tokens, positioned to provide consumers with unparalleled value on many levels. First 1554 NV hardware wallets will be assigned a unique certificate of ownership on the blockchain network in the form of NV tokens through the ERC1155 protocol, which the first 1000 lucky buyers (out of the 10,000 early adopters) will be able to mint and auction off in the future if ZVC becomes popular as a mainstream cybersecurity solution.

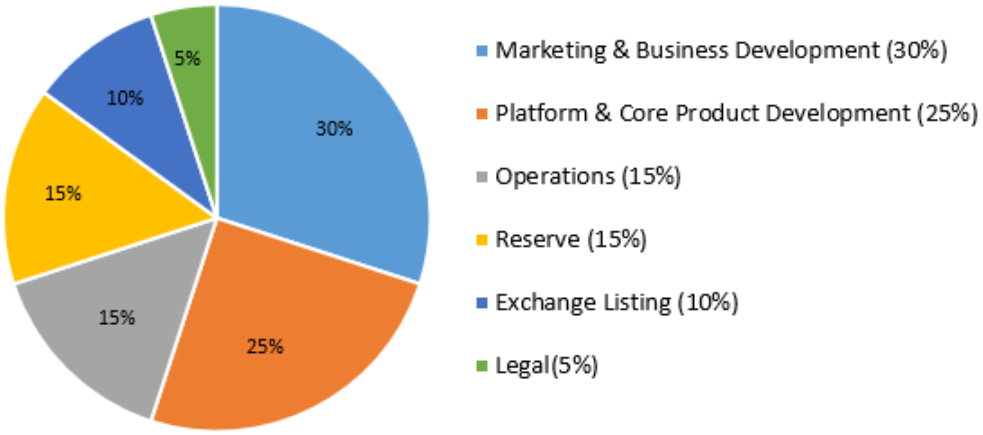
## NV CAMPAIGN

| Token Name | NatiVault |
|---|---|
| Token Symbol | NV |
| Token Type | ERC-20 Utility Token |
| Decimal Support | 18 |
| Total Token Supply | 1,000,000,000 |
| Tokens For Private & Public Sale | 44% |
| Payment Methods | BTC, ETH, USDT, USDC |

## TOKEN DISTRIBUTION



## FUND UTILIZATION




# BUSINESS MODEL

As the first hardware wallet in the world to be associated with native cryptocurrency tokens, NV Tokens would use a lean startup model to establish the business.

The NV business model is based on exciting and innovative tokenomics and incentive structures. The company has developed an innovative strategy to capture early interest of the crypto trading community with the sales of NV tokens while also achieving the anticipated first device sales. The strategy also aids in meeting the initial revenue goals.

## MARKET ENTRY STRATEGY

NV has designed a limited time early market entry to bring instant value to the worldwide community of crypto enthusiasts, traders, and influencers. Using a private sale token strategy, the project plans to generate initial funds for its development while at the same time expanding its user base.

The plan is to create awareness and initiate excitement around the brand by offering free NV hardware devices to the first 10,000 members of the community through a unique Hardware-as-a-Service model. With the purchase of NV tokens worth $100, users will receive free NV hardware wallets. With the staking of just 100 NV tokens, participants would be able to access the entire ecosystem of NV services.

Early community members would also be able to hold NV NFTs in the future, in addition to receiving hardware wallets at no upfront cost. Among the first 10,000 early adopters, 1000 lucky buyers will have the opportunity to receive NV NFTs. These NFTs are anticipated to increase rapidly in value as ZVC iterations progressively transform next-generation computing.


The launch of NV tokens would take place at the back of a HARDWARE-AS-A-SERVICE model.

An initial referral program will be launched as a part of NV promotions. The minimum buy of $100 worth NV token is capped for everyone to become NV community member. Existing members will be incentivized to expand the NV community by offering 40% referral incentives in NV tokens.

The initial business plan seeks to fulfil its immediate goal in generating enough momentum to propel the company to full-scale commercialization and expansion of this game-changing technology. Following NV token pre-sale, the company intends to launch large-scale manufacturing of NV devices and delivering pre-ordered devices to the early purchasers within the first six months of its business activity.

## MARKET CAPTURE STRATEGY

Leveraging the success of an innovative market entry strategy, NV hardware wallet will be positioned to be a market leader in the shortest possible time by:

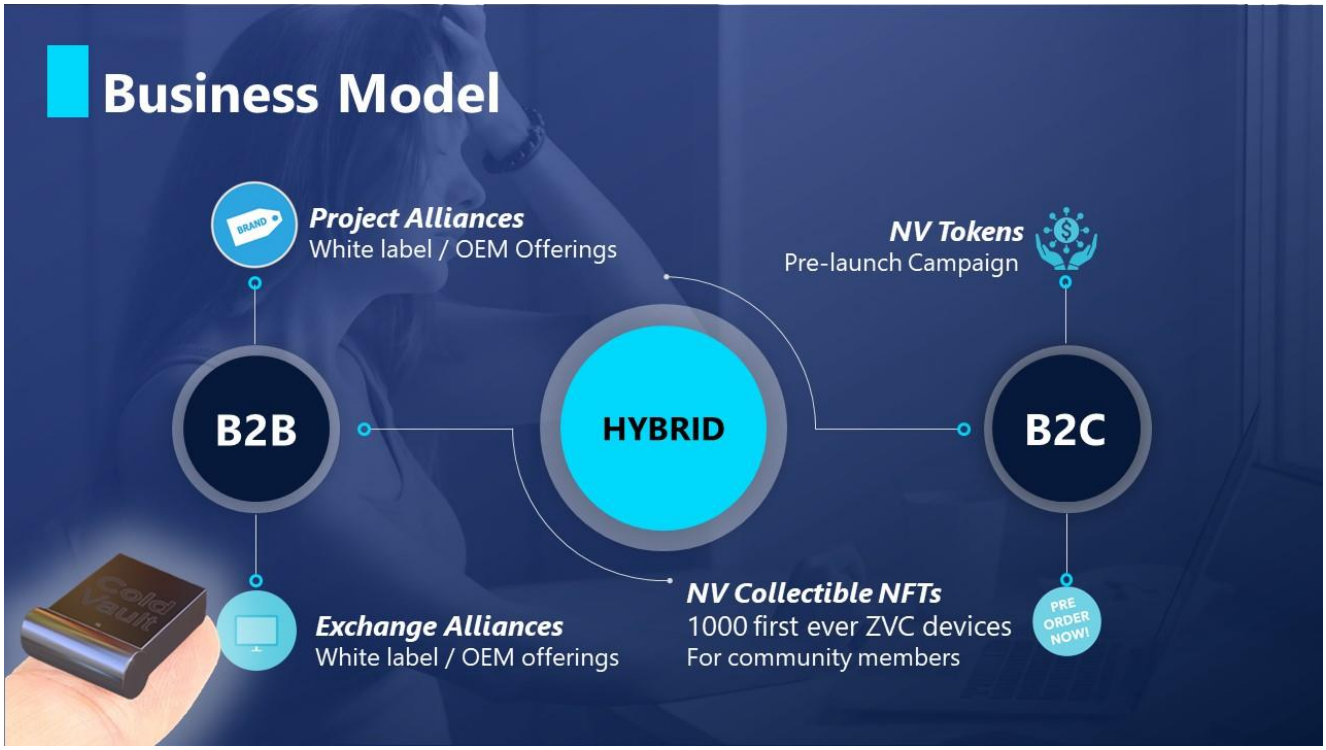
1. Adopting an aggressive and innovative global sales strategy
2. Evolving robust tokenomics model around the NV tokens and NV hardware
3. Establishing B2B relations with companies for integrating DeFi protocols and trading infrastructure.

**The NV team of scientists and researchers are presently collaborating with a leading DeFi platform with ready trading infrastructure. The infrastructure would be integrated into the NV hardware wallet ecosystem, giving NV token holders access to the widest possible financial ecosystem through NV hardware wallet.**

NV does not intend charging users for basic transaction capabilities, although they would be encouraged to store a minimum of 100 NV tokens in their wallet in order to take advantage of value-added benefits such as DeFi protocol access, and NV token rebates on DeFi or DEX transaction fees, or fees if paid in NV tokens.

B2B alliances would mutually benefit both NV and its collaborators in the DeFi space. NV can offer a wider user base while at the same time allowing its users to save money on platform transaction fees.

A prominent feature of the NV market capture strategy is incorporating crypto enthusiasts to boost device sales as well as to establish an environment that fosters the development and evolution of a robust tokenomics throughout the project cycle.




After establishing a substantial market presence in the hardware wallet and tokenomics niches, the NV business model would pursue an aggressive penetration into the multifactor authenticator (MFA) markets, all the time integrating novel elements to its ever-expanding NV tokenomics

## NV TOKEN MODEL

- **Total Token Supply: 1,000,000,000 (Limited supply of one Billion tokens only)**
- **Private sale Price (Pre-ICO): $0.01 (Limited to a hardcap of $1m)**
- **Public Sale Price (ICO): $0.1 (Limited to $20m)**

**For first 10,000 NV Devices**

A never heard of hardware-as-a-service token model awaits early adopters. 10,000 devices would be offered free of cost to the first 10,000 NV token buyers on a first-come-first-served basis. This would create excitement even as the NV community is inaugurated. Minimum investment required to become a NV community member is owning NV tokens worth $10. However, staking 100 NV tokens would offer users the following benefits:

- Wider benefits within the NV DeFi ecosystem and benefiting from additional future value-added services
- NV hardware wallet with integrated basic functionalities
- **As the ICO price of NV tokens is marked @ $0.1, a 10X return for early adopters is therefore guaranteed (limited to a hardcap target of just US$ 1m)**
- Chance to grab NV NFTs which could consequently be auctioned to get fabulous returns. Randomly picked 1000 lucky buyers out of the first 10,000 would additionally be given a chance to mint NV NFTs as and when they are introduced by the company.

**For the sale of next batch of NV devices**

The immediate utility value resides in ongoing support with a $50 worth NV token offset offered against the purchase of a $50 NV hardware wallet.*

- For each device worth $50, NV tokens worth $50 would be transferred directly into the user's NV wallet- making the device literally free!
- NV token holders will be encouraged to hold 100 NV tokens in their NV wallet to get wider access to NV DeFi ecosystem and other value-added services.
- Transaction costs incurred in utilizing the integrated DeFi platform would be encouraged to be paid in NV tokens.
- Holding 1000 NV tokens in NV wallet will make users eligible for frequent airdrops.

**NV tokens thus offered would be taken away from the liquidity pool creating shortage of tokens (as previously explained)*


## PRESALE & ICO REVENUE

**NV is the world's first and only hardware wallet backed by unique NV utility tokens.** The NV business model is built around creating a successful pre-sales campaign and further capitalizing on the initial success of the pre-sale campaign. The company intends to raise funds by launching the NV token sales in 2 stages:

Proceeds from the NV token presale would be utilized to commence incorporation of NATIVAULT LIMITED (UK), commence business development operations and aggressively pursue product development and technology validation activities.

**In association with THE UNIVERSITY OF PIRAEUS (SecLab), NV is organizing an open hackathon challenge for developers to establish an iron-clad proof and endorsement of the technology. The university has signed a letter of intent to support the initial testing of technology by organizing a security challenge as a part of their ongoing national and international cybersecurity ANTI HACKING exercises.** (Letters of intent can be found on our website)

**Private Sale Base Price: $0.01**

**NV Presale details:**

| Token Price | Soft Cap | Hard Cap | Max Tokens Allotment | % Allotment |
|---|---|---|---|---|
| $0.01 | $500,000 | $1,000,000 | 100,000,000 | 10% |

**NV Public Sale (ICO):** Capitalizing on the initial success of NV Presale, NV Public Sales is planned beyond 6 months from the date of presale and will attract investments while at the same time building an Advisory panel, a wider community of NV collaborators, early and late adapters, investors, and product users.

The following are the preliminary details of the NV Public Sale (ICO):

**Public Sale (ICO) Base Price: $0.1**

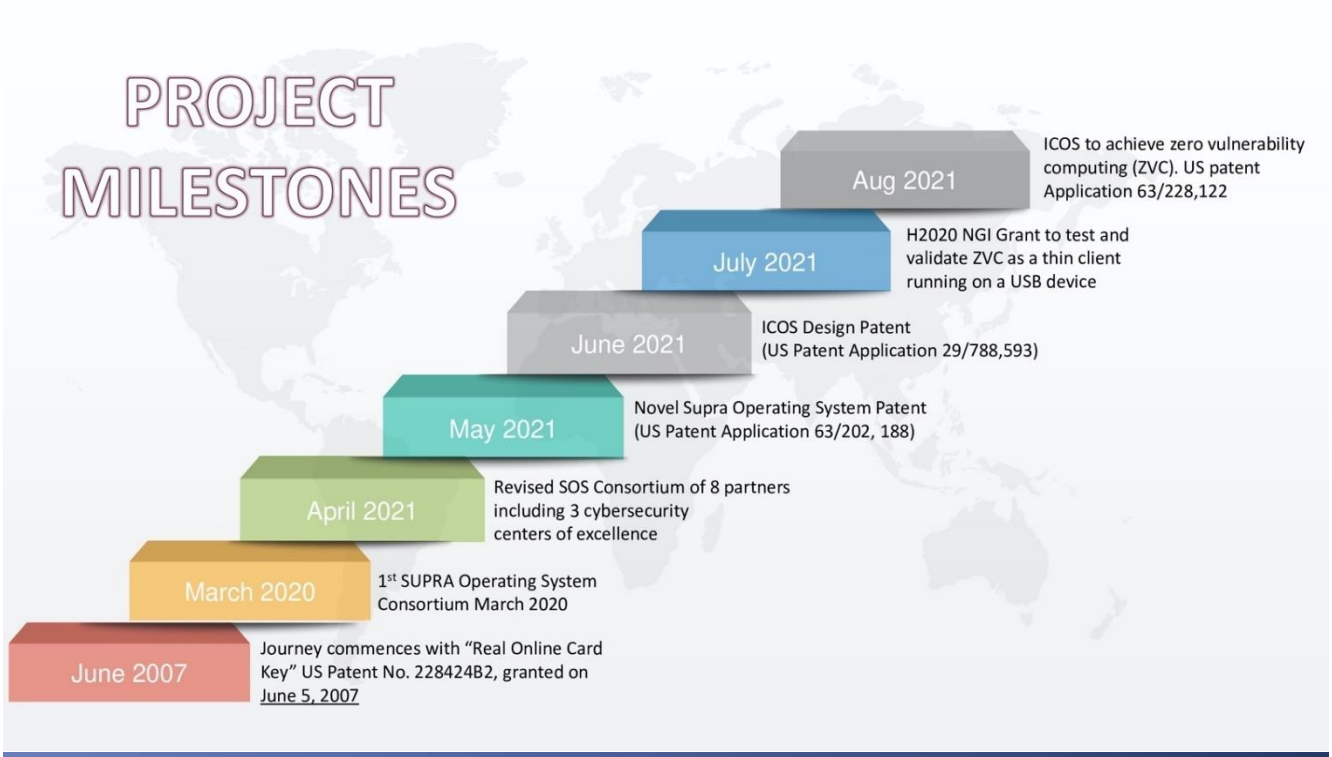
The Public ICO activities would run in 5 phases. NV tokens would be offered to buyers at discount rates tied to meeting of corporate objectives. The strategy is designed to incentivize early adopters in an open and transparent manner.

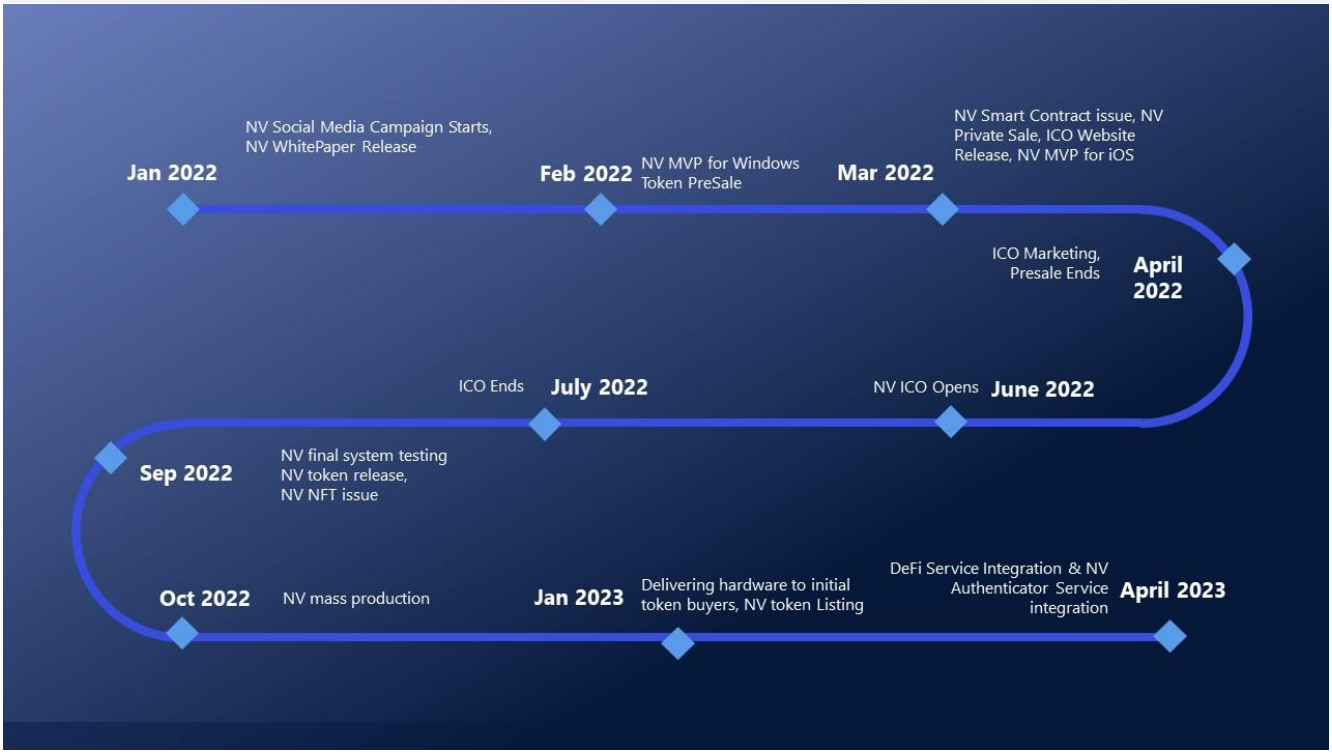
| Public Sale | Discount Rate (%) | Discount Price ($) | Hard Cap ($) | Vesting Period (months) | Token Allocation (%) |
|---|---|---|---|---|---|
| Sale 1 (2days) | 70% | 0.03 | 2,000,000 | 12 | 6.67 |
| Sale 2 (5days) | 50% | 0.05 | 3,000,000 | 10 | 6 |
| Sale 3 (7days) | 40% | 0.06 | 4,000,000 | 8 | 6.67 |
| Sale 4 (10days) | 30% | 0.07 | 5,000,000 | 6 | 7.14 |
| Sale 5 (14days) | 20% | 0.08 | 6,000,000 | 3 | 7.5 |
| **Total** | | | **20,000,000** | | **33.98** |

## PROJECT MILESTONES

NatiVault is the culmination of our efforts in the Cybersecurity space commencing with a 2007 patent that entailed a Real Online Card Key (ROCK) device that bypassed the computer OS by running a thin OS on a CD ROM to execute an online transaction. (US Patent No. 228424B2, granted on June 5, 2007, submitted on August 12, 2002.) Over the years, we formed an EU Consortium of 10 members, including three Cybersecurity Centres of Excellence, who have provided the initial validation for the technological milestone.

NatiVault's Zero Vulnerability Computing solution got its first real-world validation when it was awarded a Horizon 2020 NGI grant. NV's major milestones are furnished below:



# THE TEAM

NatiVault is a first-to-market hardware wallet developed by NV's Estonia-based holding company Blockchain 5.0 Ltd (BC5).

BC5 has over two decades of experience in researching and developing cybersecurity and Internet of Things (IoT) devices. The company has a stronger presence in the EU Horizon 2020 domain, having worked on many projects with over 40 EU Partners and earned three H2020 Funded Grants in the last two years.

**BC5 holds the patent rights of the ZVC technology and would license it to NatiVault Ltd, an independent legal entity to be registered in UK. NatiVault Limited would hold exclusive rights to commercialize NV hardware wallets and authenticators as the first use cases based on the ZVC technology, as well as developing and promoting NV tokenomics.**

NatiVault is led by an experienced team of blockchain, DeFi, technology, marketing, e-commerce, finance, and EU relations professionals. It is not just NatiVault's grounding in technology, its diverse background, or its knowledge of blockchain networks and cryptocurrencies that give NV depth and substance. Our team is dedicated to building a company legacy born out of an unstinted commitment to do what is good for the world and its people.

NatiVault would empower NV customers, DAO members and stakeholders to realize the true worth of their assets riding on a unified philosophy born out of 3 distinct commitments:

1. Path breaking innovation designed to transform cybersecurity forever,
2. Unquestionable ethics and code of conduct, as well as
3. Unrivalled customer service.


## PARENT COMPANY HOLDING ZVC IP:

BLOCKCHAIN 5.0 LTD (ESTONIA)

## REAL ONLINE CARD KEY TECH DEV. PARTNER:

ZEROMILE R&D LLP (INDIA)

# CONTACT DETAILS

The NatiVault ecosystem is always growing, and our team values collaboration, feedback, and foresight. You are welcome to get in touch with us:

| | |
|---|---|
| Website | NatiVault |
| Email | info@nativault.com |
| Medium | https://medium.com/@nativault |
| LinkedIn | https://www.linkedin.com/in/nati-vault-05b856227/ |
| Twitter | https://mobile.twitter.com/nati_vault |
| Reditt | https://www.reddit.com/r/NatiVault/ |
| Instagram | https://www.instagram.com/nativault/ |
| Facebook | https://www.facebook.com/Nativault-110598278082135/ |
| Discord | https://discord.com/invite/BQBTY7gA |
| Telegram | https://t.me/NatiVault |