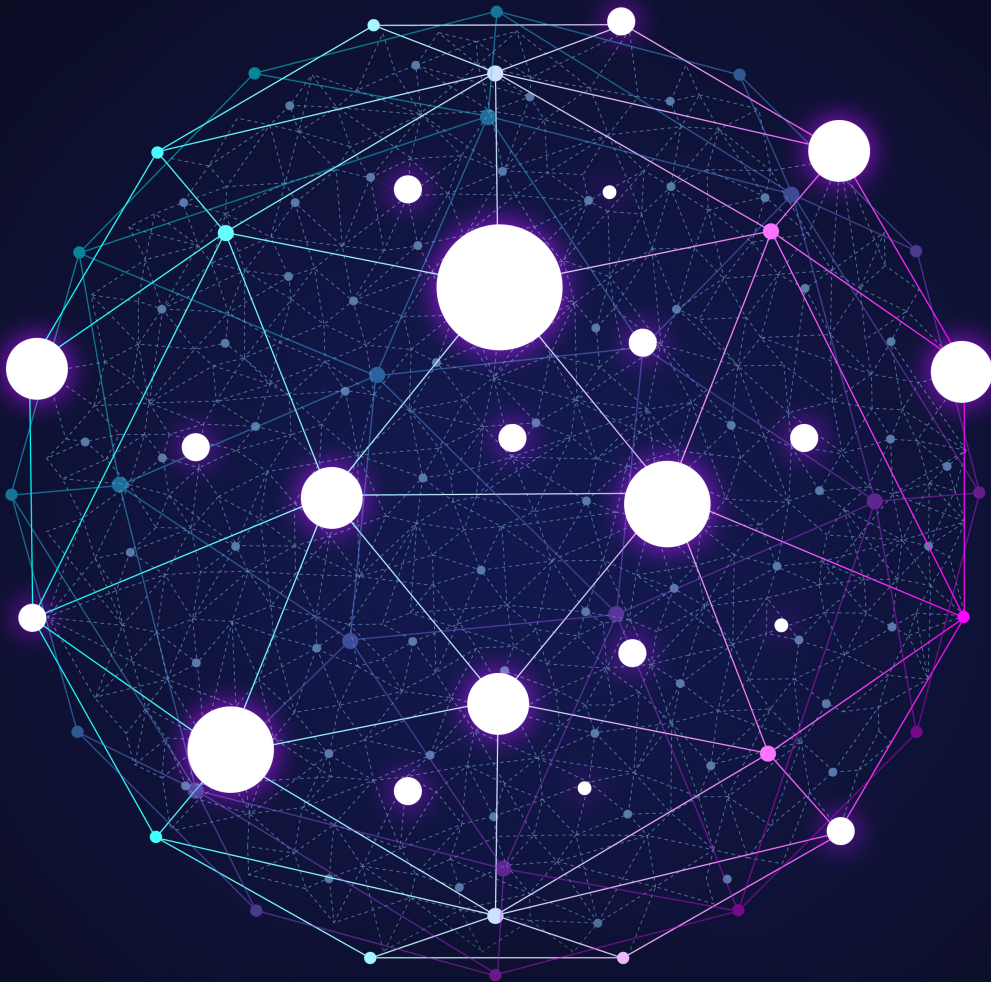


# MPando Browser Tech Book

---



# Contents

## 1. MPando Browser Tech Book

1.1 Shortcomings of Existing Browsers

1.2 MPando Browser & Web 3.0

## 2. MPando Browser Highlights

2.1 SmartBlock

2.2 HTTP Referrer Protection

2.3 Internet Engineering Task Force (IETF) Certified Encryption Technology

2.4 Private Browsing Mode

2.5 Built-in Functionalities

2.6 Portability

2.7 Add-ons for Convenience

# 1.1 ————— Shortcomings of Existing Browse

It has been little under 30 years since the first commercialization of the Internet, and nearly 4.6 billion people, roughly 60% of the world population, are now using it. As such, the Internet has an immense influence across the economy, society, and culture.

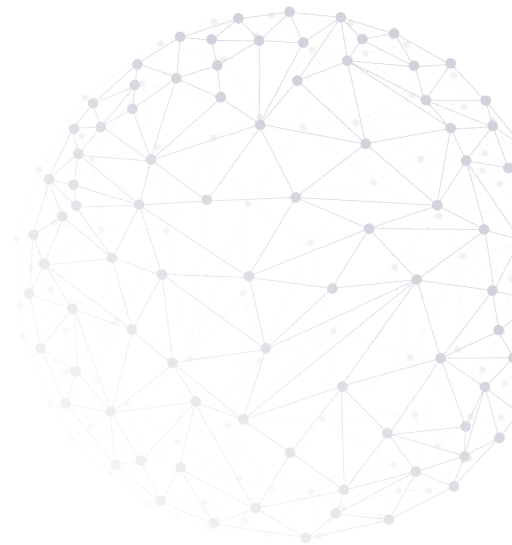
Internet’s accelerated growth can largely be attributed to the World Wide Web and web browsers. Web browsers are graphic user interface software programs that communicate with web servers and output HTML documents and files.

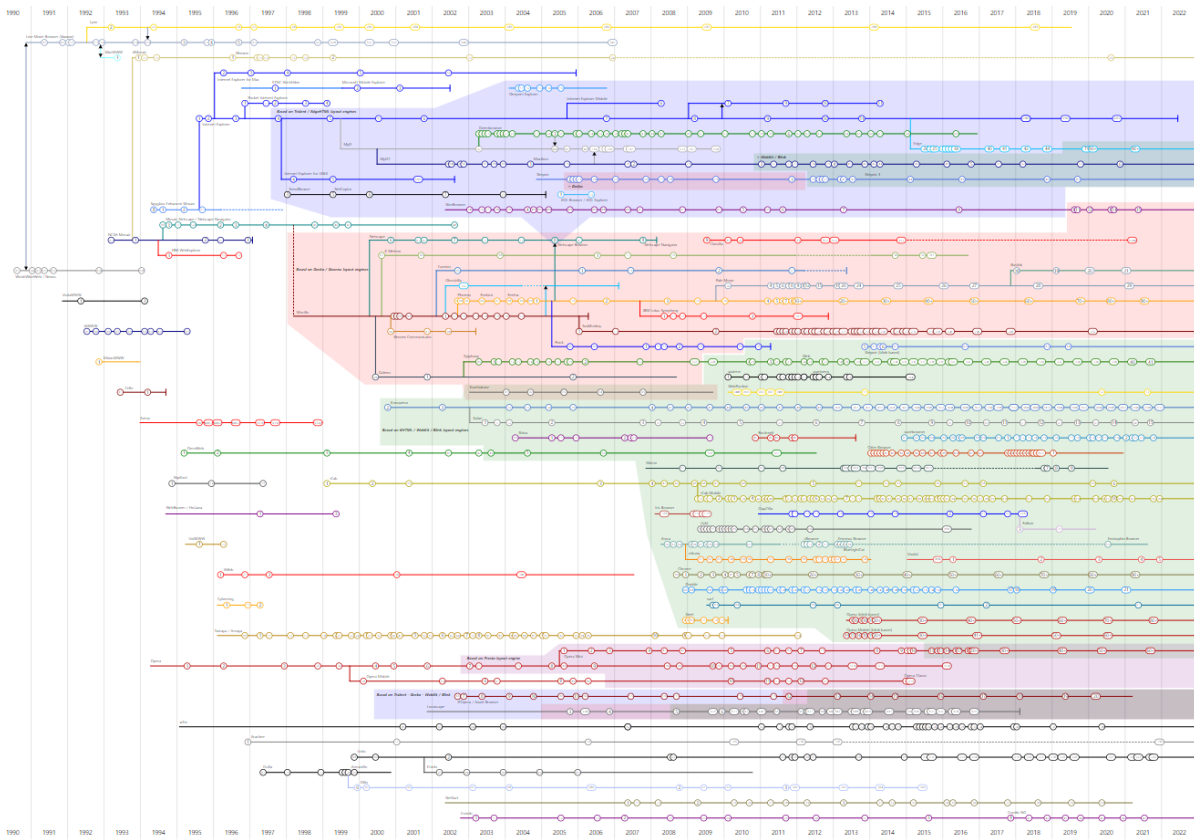
Starting from the early stages of the Internet adoption in 1991 until now, many software developers have been improving the performance of browsers and adding new functionalities to provide satisfactory web experience to users. That being said, the development history of web browsers in the market is the history of fierce competition among software companies. Often referred to as the Browser Wars, the competition brought about the positive effects of accelerated technological advances, but at the same time, resulted in the critical side-effect of fragmentation. Web pages or apps written in identical codes failed to be compatible in various browser environments, and often had to be adjusted to each environment.

While users expect the same kind of experience regardless of which browser they use, the reality is that different browsers show different outputs or actions. This alone sometimes serves as the deciding factor for many users.



<Major Web Browsers>





<Web Browser Timeline>

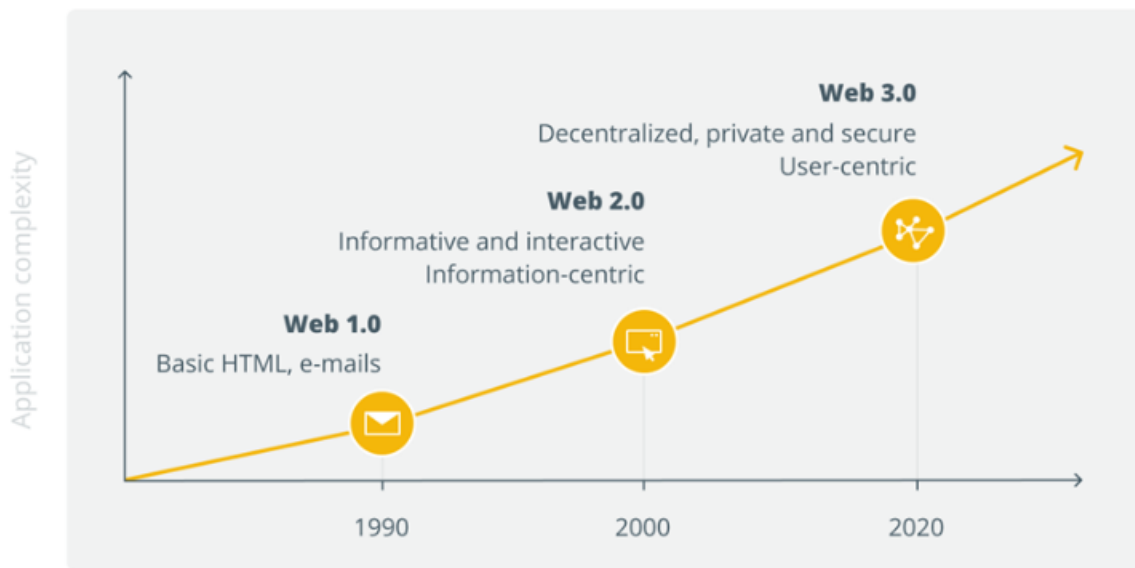
Software companies have been making continuous efforts for a standardized web to remedy fragmentation. The major web standards, such as HTML, CSS, and ECMAScript, have been revised and updated constantly, and browser companies are keeping up with them. However, in the web standardization process, there have been differences in the desired directions that resulted in splits of such standards. Still, fragmentation, where web standard compliant codes are not compatible across browsers, remain to be resolved.

As of January 31, 2020, Internet Explorer (IE) 10, along with Windows 7, have gone out of support by Microsoft. In addition, IE11, too, is scheduled to be retired. Microsoft offers Edge as the new official browser, but it does not have much competitive edge against other browsers.



# 1.2 ————— MPando Browser & Web 3.0

MPando Browser provides personalized services to each user by taking advantage of Web 3.0, the intelligent Semantic Web technology that interprets the contents of a webpage.



<History of the Internet>

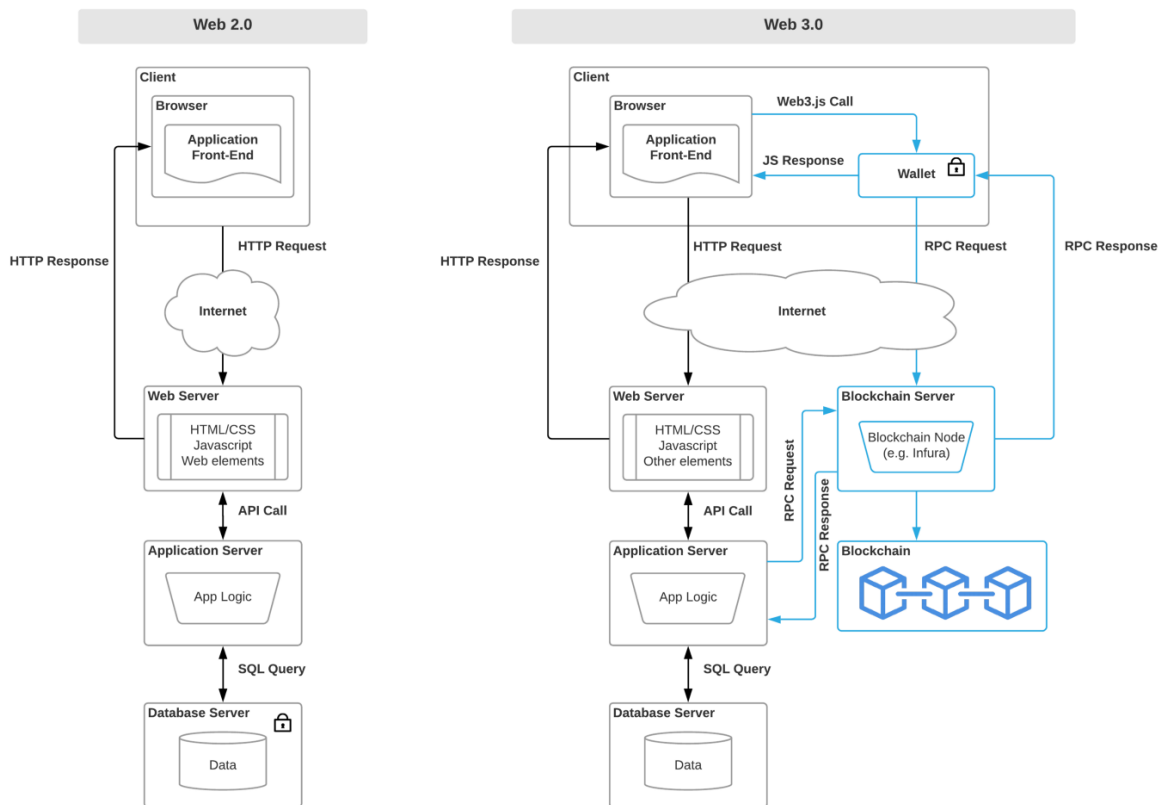
Web 2.0, marked by SNS websites such as Facebook, Twitter, and LinkedIn, as well as instant messaging services such as WhatsApp, WeChat, and KakaoTalk, is unable to link the massive volume of fragmented information.

Tim Berners-Lee has invented the intelligent web by semanticizing every datum in existence on the web, and the Semantic Web technology that constructs a web environment in which computers can quickly and automatically process information without human input.

Developed on the basis of Semantic Web technologies are ontologies and metadata - and based on these technologies is the Web 3.0 era.

Web 3.0 is a newly established ecosystem that utilizes some of the attributes of the blockchain technology. It is constituted by over 3,000 Decentralized Applications (Dapps).

Dapps are, as the name suggests, decentralized applications with no central authority. They have the role of maintaining the network but no controlling power. As a result, users retain the full ownership of their own data, and for those who decide to share their data can gain financial rewards through their digital profiles.



<Web2.0 & Web3.0 Application Architecture>

Since MPando Browser is built based on Web 3.0, it offers the advantages of decentralization.

No longer in need of a middleman, MPando Browser provides a platform where transactions can be made securely without a third party. Blockchains like Ethereum require validations from the users and make it impossible to break the rules with their data encryption.

With the MPando Browser, neither governments nor institutions have control over users' data, and no individual has control over the identity of others. This reduces the risk of government or corporate censorship and makes it less susceptible to denial-of-service attacks (DoS, which maliciously attacks a system to run out of resources to prevent access to the network).

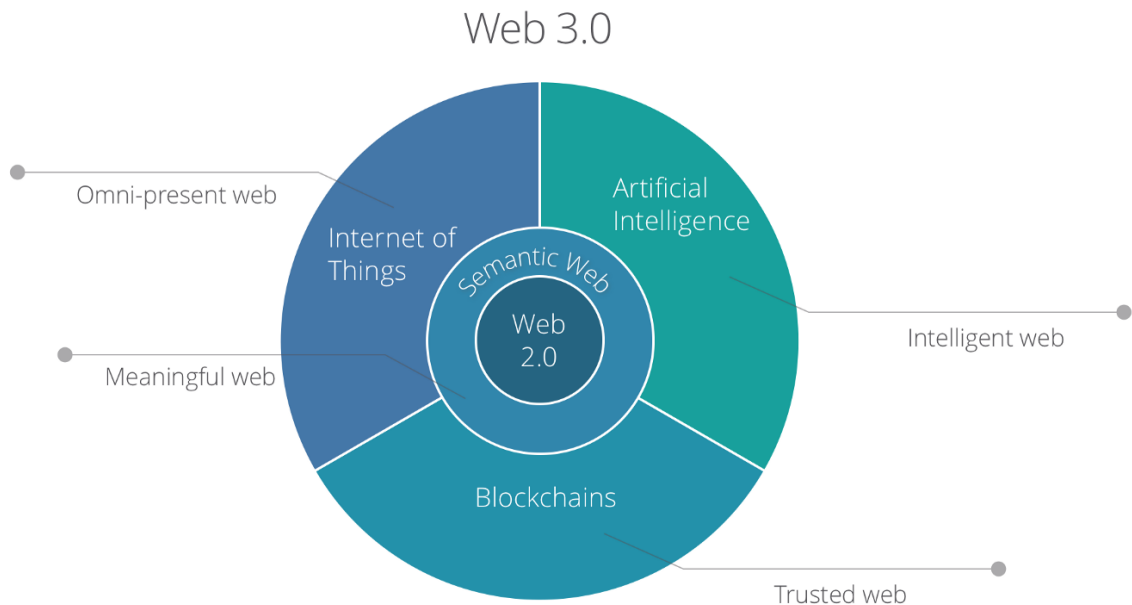
Users regain 100% of their rights to their data, and the data are encrypted and protected. Other companies cannot freely use metadata such as personal preferences, income, diet, and interests. Since stored data is decentralized and distributed, hackers will have to hack the entire network, drastically decreasing hacking and data leakage.

Based on Web 3.0 technologies, it is easy to customize the applications, and they can be executed regardless of devices such as smartphones, automobiles, TVs, microwave ovens, and smart sensors. As more and more products are connected to the Internet, larger sets of data provide algorithms with more information to analyze. This allows for more efficient browsing by helping provide accurate information that meets the specific needs of individual users.

In the past, it was quite difficult to get desired results through search engines. But over the years, search engines have come to find semantically relevant results based on search content and metadata. This naturally transitioned into a more convenient web browsing experience that makes it relatively easy for anyone to find the exact information they are looking for.

An efficient algorithm can filter out search results manipulated by Artificial Intelligence (AI). Anyone will be able to create an address and interact with the network, allowing wealth and digital assets to be transferred efficiently, quickly and securely across the globe. Furthermore, uninterrupted services can be provided, significantly reducing account suspensions and service delays.

Because there is no single point of failure (SPOF), service failures are minimized. Thanks to data stored redundantly on distributed nodes, multiple backups are ensured. This results in better responses to server failures and seizures.



<Convergence of AI, IoT (Internet of Things), and Blockchains>

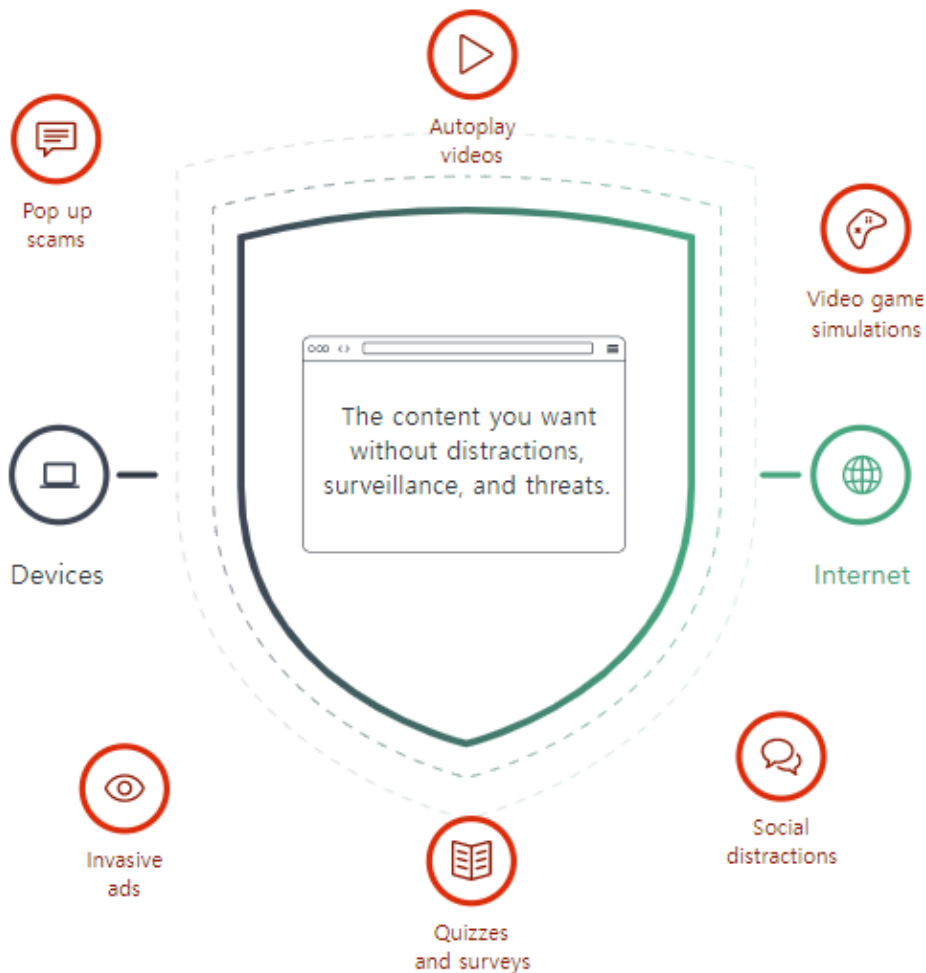
The benefits of Web 3.0 technologies reach many aspects of advertising and marketing. Hardly anyone is a fan of indiscriminating online advertisements, but there is a fine line of distinction between a barrage of irrelevant advertisements and useful advertisements. By using an advanced AI system to improve advertising, Web 3.0 is able to target specific audiences based on consumer data.

MPando Browser provides better customer service. Customer service on websites and web applications is key to a seamless user experience, but the sheer cost prevents many successful web services from scaling customer service accordingly. However, MPando Browser utilizes a smart chat bot that can communicate with multiple customers at a time, allowing users to enjoy better services than from a service agent.

# 2.1 SmartBlock

With personal browsing and enhanced tracking protection, the MPando Browser goes to great lengths to protect web browsing activities from trackers. As part of this, built-in content blocking functionality automatically blocks third-party scripts, images, and other content from being loaded by an intersite tracking company reported by Disconnect.

This type of aggressive blocking can sometimes cause minor inconveniences, such as missing images or performance degradation. On rare occasions, this could result in malfunctioning or blank pages.



<Disconnect Tracking Protection>

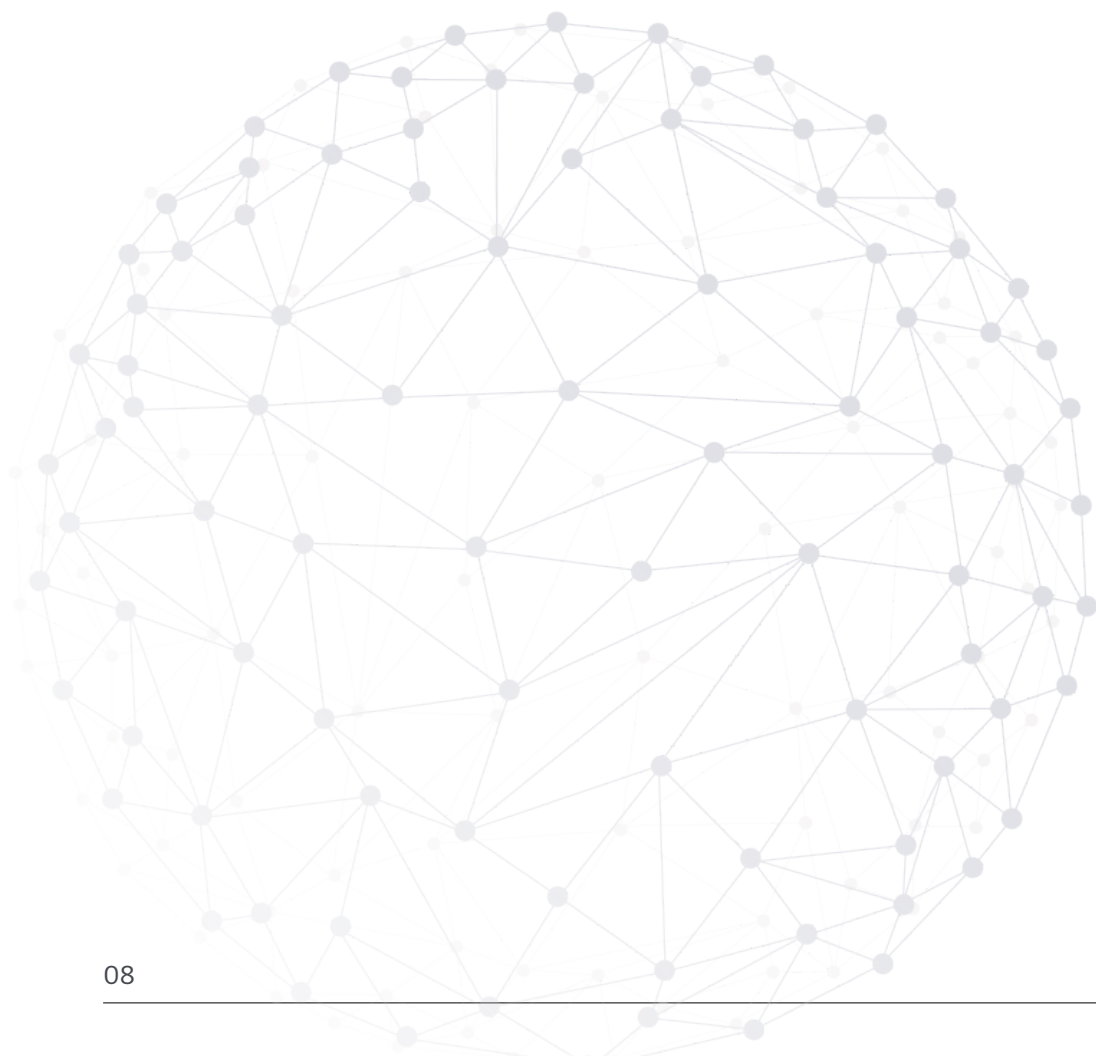
As a preventive measure, we developed SmartBlock, a mechanism that intelligently loads a local privacy alternative to a blocked resource that works well enough like the original resource to ensure that a website is working properly.

SmartBlock is a tracking protection function that intelligently corrects malfunctions or blank pages without compromising user privacy. It also provides a local alternative of the blocked third-party tracking scripts to take corrective action.

These standalone scripts behave just like the scripts from the source, which allows for functionality verification for the website. With this feature, corrupted sites that rely on existing scripts can be loaded in their original state.

The third version of SmartBlock greatly improves support for substituting the popular Google Analytic scripts and adds support for popular services such as Optimizely, Criteo, Amazon TAM, and various Google advertising scripts.

This substitutive feature of SmartBlock is bundled with the MPando Browser, and since no third-party content from the tracker is loaded, it cannot track users in any way.

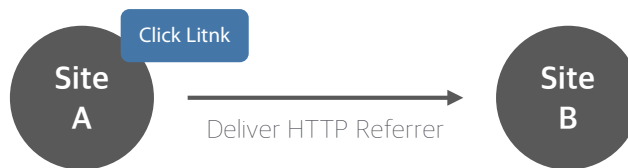


# 2.2 HTTP Referrer Protection

The HTTP Referrer header refers to the traces of visited websites via hyperlink when surfing the web using a web browser.

This header contains the following: the absolute or partial address of the page that sent the current request; the address of the webpage that contains the link if arriving via the link; or the address of the webpage with the requested resource.

Such headers are often used by websites for analysis, logging, and cache optimization. However, this is where the problem arises. If the browser sends the entire URL of the previous website, the URL may expose sensitive user data. Some sites may want to avoid being addressed in the Referrer header.



The Referrer policy was introduced to resolve this issue.

Websites can control the value of the Referrer header, allowing stronger privacy protection for users.

MPando Browser goes a step further and sets a new default Referrer policy to Strict-origin-when-cross-origin for a more robust protection of user privacy when sharing with other websites.

This is because only the origin value is passed to the Referrer in case of a cross-origin request. Therefore, it prevents the possibility of leakage of personal information included in URL paths and query strings.



With the release of Version 93, MPando Browser disregards the relatively less restrictive Referrer policies for cross-site requests such as 'no-referrer-when-downgrade,' 'origin-when-cross-origin,' and 'unsafe-URL.' This prevents the possibility of personal information being leaked.

If the Referrer policy is not set, the existing policy of MPando Browser is applied. In other words, MPando Browser always trims the HTTP Referrer for cross-site requests, regardless of the website's settings.

For the same site requests, the website as well as the full Referrer URL can be transmitted.

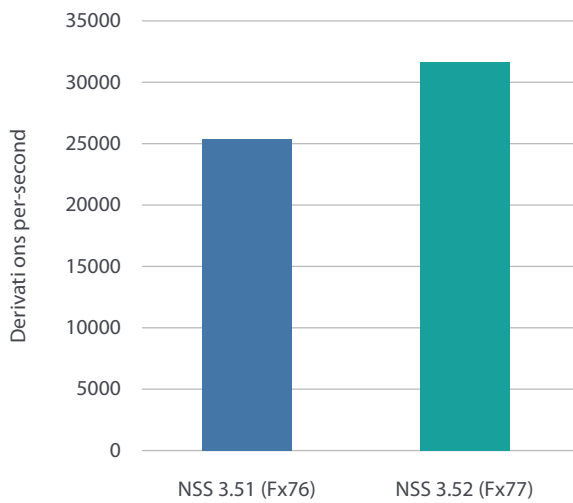


# 2.3 Internet Engineering Task Force (IETF) Certified Encryption Technology

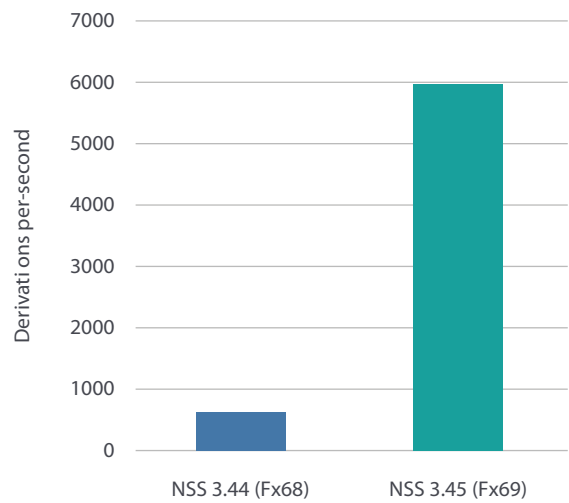
For the core setting, we recently replaced the 32-bit implementation of Curve25519 with the implementation of the Fiat-Crypto project. The arbitrary-precision arithmetic function in this implementation has proven to be functionally correct and tenfold improvement over the existing code.

MPando Browser has been updated with the new HAACL\* code to implement 64-bit, achieving up to 27% speed improvement compared to the previous version. MPando Browser recently brought this update to Windows as well.

Improvements like these are very important. As for telemetry, Curve25519 forms the most widely used elliptic curve for ECDH(E) key setting of MPando Browser, and when applied to mobile devices, energy consumption is reduced compared to increased throughput, which is a particularly important factor in mobile devices.



<64-bit Curve25519(with HAACL)>



<32-bit Curve25519 with Fiat-Crypto>

The arithmetic properties of Curve25519 are as follows.

$$y^2 = x^3 + 48662x^2 + x$$

The curve used is the Montgomery curve over the fractional domain defined by the prime number of  $2^{255} - 19$ . This reference point creates a circular subgroup of prime numbers. This subgroup represents the following prime number:

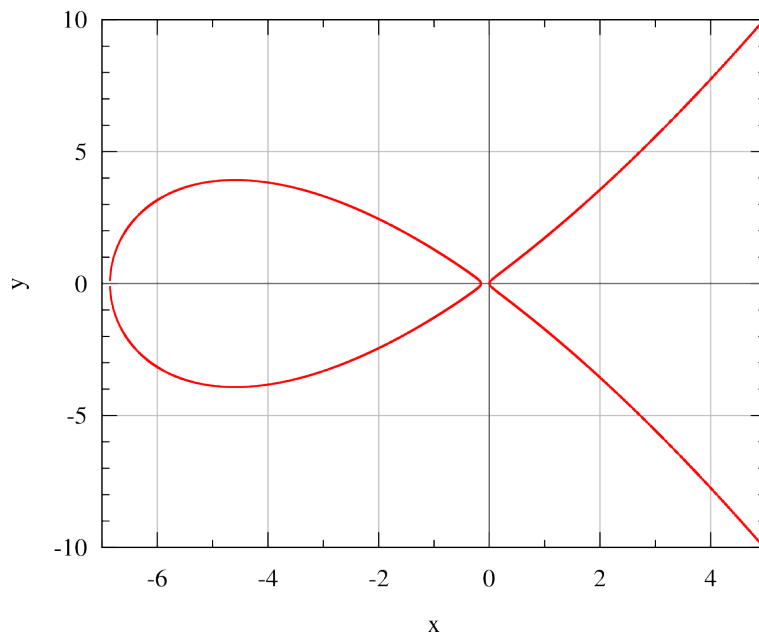
$$2^{252} + 27742317777372353535851937790883648493$$

The co-factor of the subgroup is 8, which means the number of elements in the subgroup is  $1/8$ .

The Montgomery curve over field  $K$  is defined by the following function:

$$M_{A,B} : By^2 = x^3 + Ax^2 + x$$

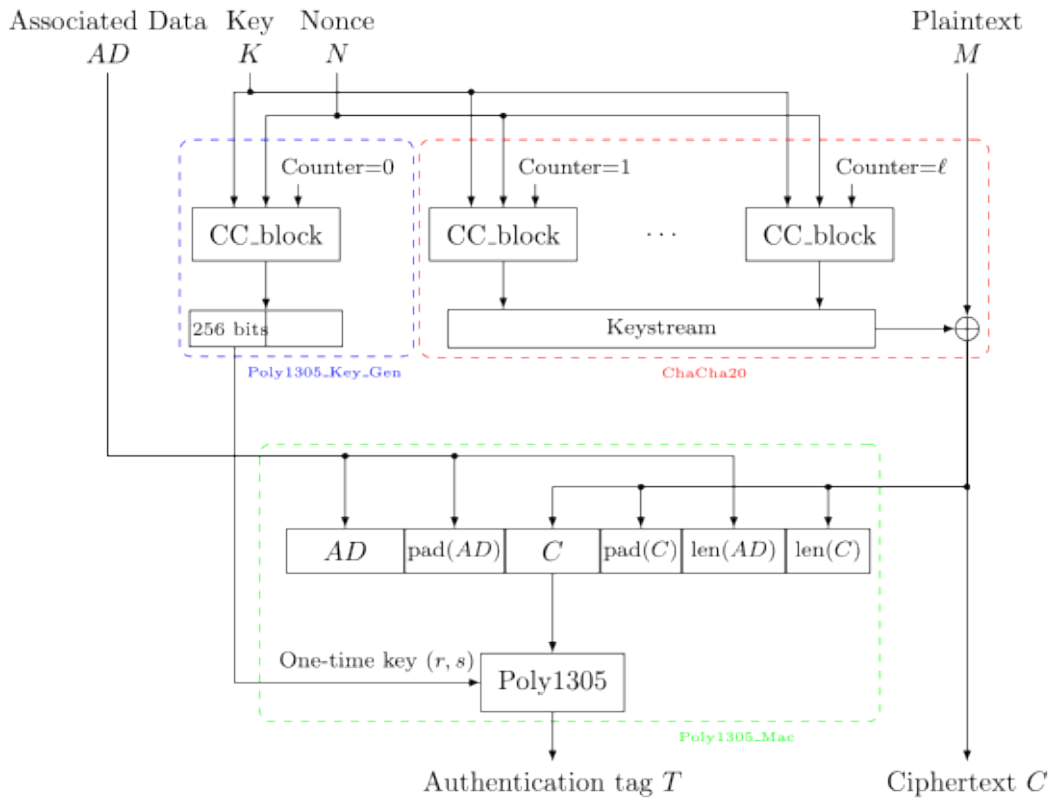
for certain  $A, B \in K$  and with  $B(A^2 - 4) \neq 0$



<curve25519 Montgomery curve>

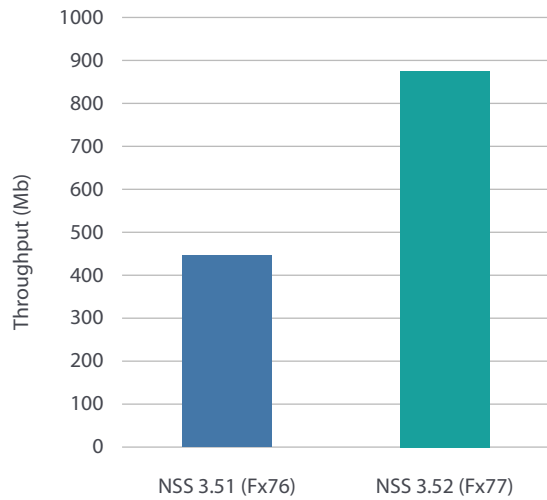
MPando Browser improved the performance of ChaCha20-Poly1305 for encryption and decryption.

ChaCha20-Poly1305 is an Authenticated Encryption with Additional Data (AEAD) algorithm that combines a ChaCha20 stream cipher with a Poly1305 message authentication code.



The ChaCha20-Poly1305 algorithm generally outperforms the popular AES-GCM algorithm, which is often used on systems with CPUs that do not support hardware acceleration.

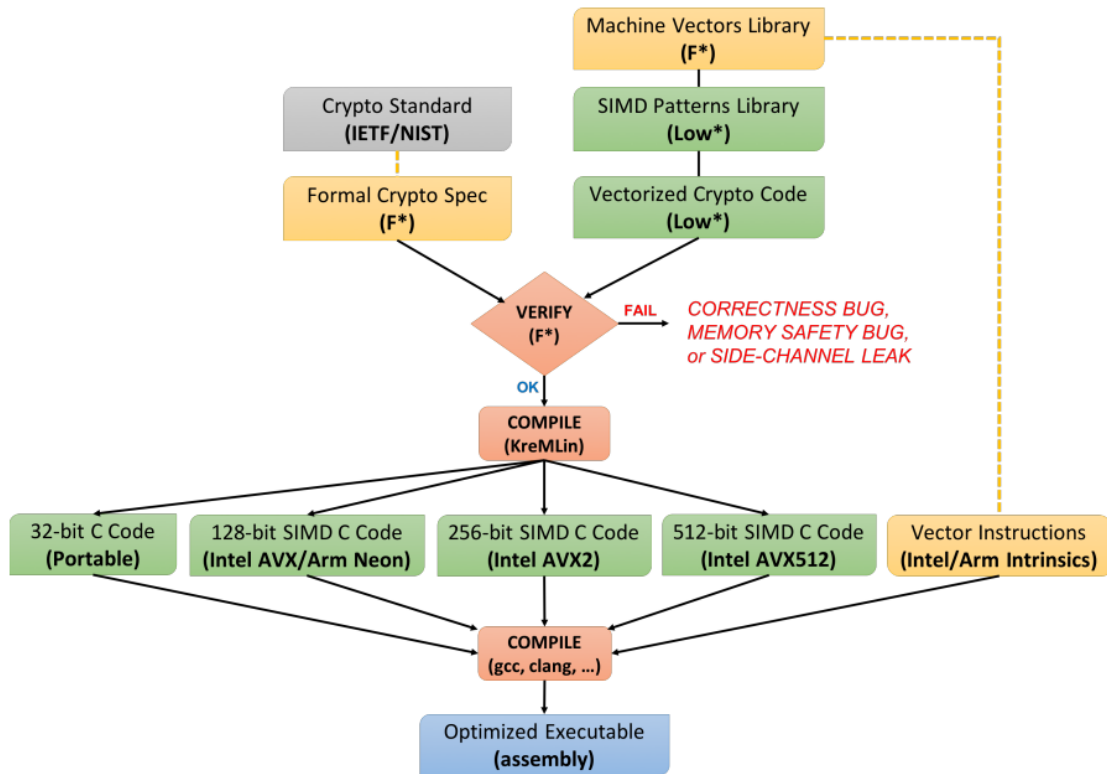
Utilizing vectorization with 128-bit and 256-bit integer arithmetic (using AVX2 instructions set on x86-64 CPUs), throughput doubled. If these features are not available, NSS will fall back to AVX or Scala implementations, both more optimized.



<ChaCha20-Poly1305 with HACL\* and AVX2>








The HACL\* project has introduced new techniques and libraries to improve efficiency in writing verified primitives for both scalar and vectorized variants.

This allows for aggressive code sharing and reduces verification efforts across multiple platforms.



<HACL Programming and Verification Workflow>

# 2.4 Private Browsing Mode








보안 및 개인 정보 보호							
프라빗 브라우징 모드	✓	✓	✓	✓	✓	✓	✓
기본적으로 타사 추적 쿠키 차단	✓	—	✓	✓	✓	✓	✓
크립토마이닝 스크립트 차단	✓	—	✓	—	✓	✓	—
소셜 트래커 차단	✓	—	✓	✓	—	✓	—

It is not impossible to expect and trust high levels of data protection and privacy in the browsers we use to access the Internet regularly.

For instance, the Private Browsing mode of the MPando Browser automatically deletes traces that remain locally, such as browsing and search history, as well as other inputs.

In addition, other traces such as bookmarks and downloads that users need are protected.

# 2.5 Built-in Functionalities

공익 사업							
자동재생 차단	✓	—	✓	—	—	✓	—
탭 브라우징	✓	✓	✓	✓	✓	✓	✓
북마크 관리자	✓	✓	✓	✓	✓	✓	✓
자동으로 양식 작성	✓	✓	✓	✓	✓	✓	✓
검색 엔진 옵션	✓	✓	✓	✓	✓	✓	✓
텍스트 음성 변환	✓	—	✓	✓	—	—	✓
리더 모드	✓	✓	✓	✓	—	✓	✓
맞춤법 검사	✓	✓	✓	✓	✓	✓	✓
웹 확장/추가 기능	✓	✓	✓	✓	✓	✓	✓
브라우저 내 스크린샷 도구	✓	—	✓	—	✓	—	—








In addition to privacy protection, which typically occurs in the background of the browser, other crucial elements of a well-crafted browser are the user interface and functionality.

The MPando Browser offers features that Chrome, Safari, Opera, and Internet Explorer do not support, including automatic playback blocking, text-to-voice conversion, and native screenshot tools. Processing speed is also faster and safer.



# 2.6

## Portability

휴대성							
OS 가용성	✓	✓	✓	—	✓	✓	—
모바일 OS 가용성	✓	✓	✓	—	✓	✓	—
모바일과 동기화	✓	✓	✓	✓	✓	✓	—
비밀번호 관리	✓	✓	✓	✓	✓	✓	✓
기본 비밀번호	✓	—	✓	—	✓	—	—

In an era of nearly 5 billion Internet users worldwide, portability is the most important factor in choosing a web browser. It is noteworthy that not all browsers support all operating systems. In other words, some web browsers are not available depending on the operating system.

Firefox, Chrome, Edge, Brave, and Opera work on all major systems and are easy to install, while Internet Explorer and Safari only work on Microsoft and Apple's own systems. Apple's mobile devices come pre-installed with Safari, and most Android devices come pre-installed with web browsers modified by the manufacturer.

However, the MPando Browser can easily be installed and is available on all operating systems and devices, just like Firefox, Chrome, Brave, Edge, and Opera.

The MPando Browser supports synchronization between desktops and mobile devices that most web browsers support. By installing the MPando Browser on multiple devices and logging in, users can enjoy the benefits of securely synced convenience features such as saved passwords, browsing history, bookmarks, and settings across all the devices.

# 2.7 — Add-ons for Convenience

The MPando Browser offers various add-ons as convenience features for users to easily install and configure. These add-ons help users customize their Internet browsing experience to their tastes. The add-ons provided by the MPando Browser allow user to use a wider range of unique services offered by Pando Software.

