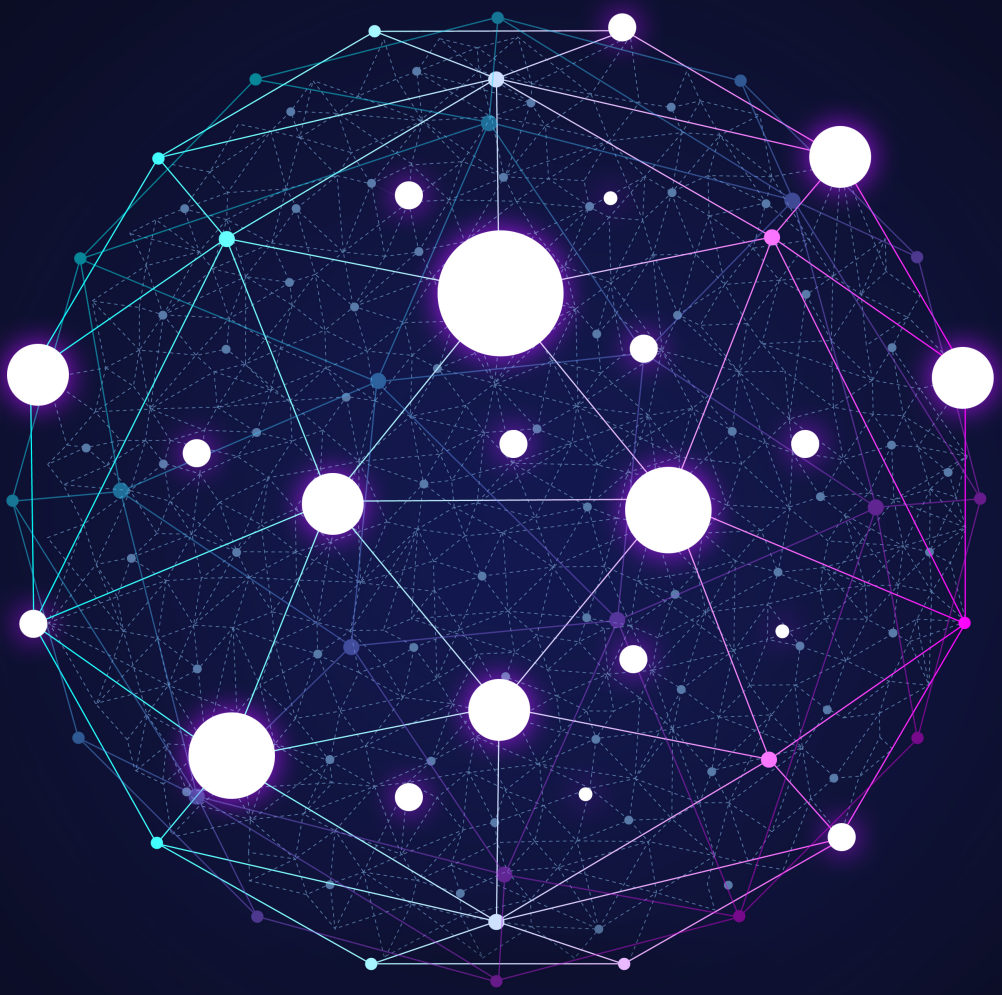
MPando Browser
Tech Book



Contents

1.1 기존 Web Browser 의 문제점

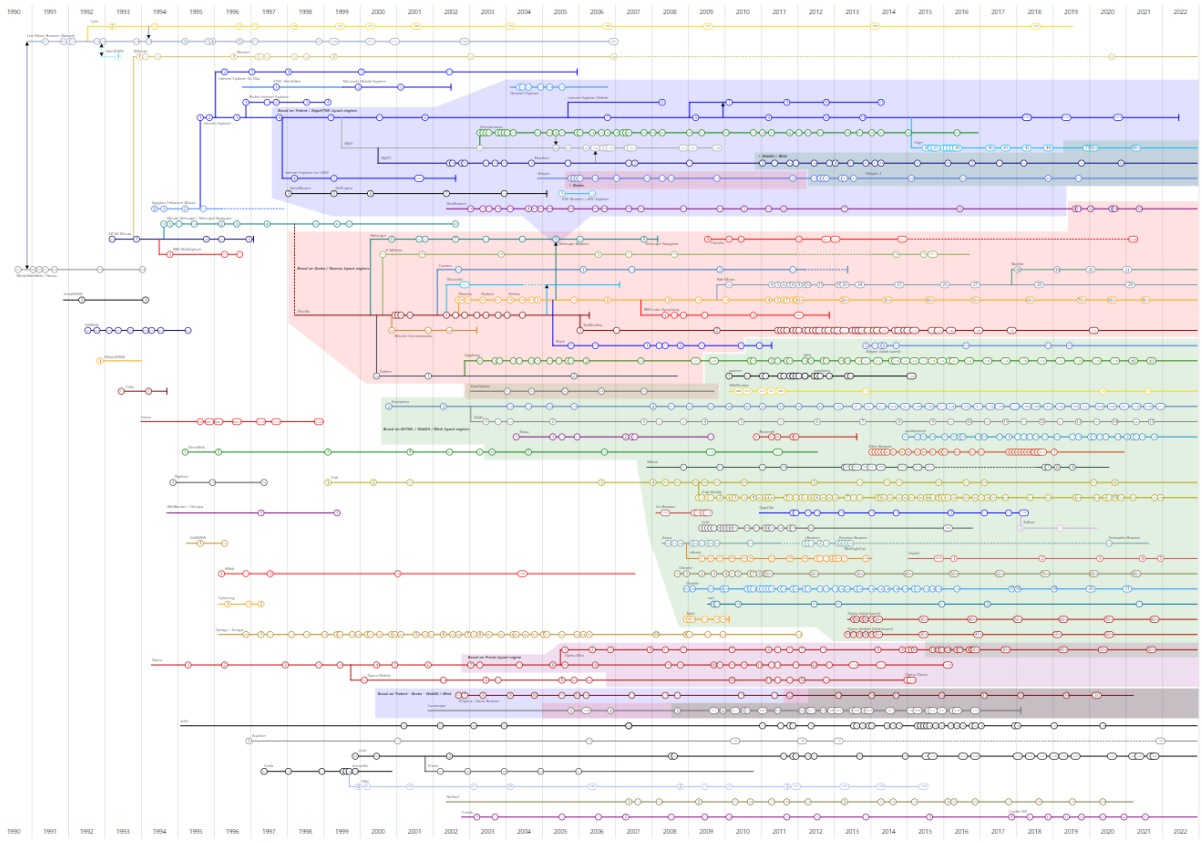
Internet이 전 세계적으로 상용화된 지 30년이 안 되었지만, 현재 인터넷을 이용하는 사람은 전 세계 인구의 60%에 달하고 이는 46억 명에 이릅니다. 이에 따라 경제, 사회, 문화 전반에 걸쳐 인터넷이 막대한 영향을 끼치고 있다고 해도 과언이 아닙니다.

인터넷이 급성장할 수 있었던 배경을 살펴보면 월드와이드웹(World Wide Web)과 웹 브라우저(Web browser)의 역할이 컸습니다. 웹 브라우저는 웹 서버에서 이동하며 쌍방향으로 통신하고 HTML(Hyper Text Markup Language) 문서나 파일을 출력하는 그래픽 사용자 인터페이스 기반의 응용 소프트웨어입니다.

웹이 태동하기 시작한 1991년부터 지금까지 만족도 높은 웹 경험을 사용자에게 제공하기 위해 다수의 개발사들이 기능과 성능을 꾸준히 개량하고 있습니다. 또한 웹 브라우저의 발전 과정을 살펴보면 시장 점유 우위를 차지하기 위해 소프트웨어 회사들이 벌인 치열한 경쟁의 역사라고 볼 수 있습니다. 이를 브라우저 전쟁(Browser Wars)로 부르는데, 이 전쟁에는 기술 발전 속도를 높이는 긍정적인 효과가 있었으나 동시에 파편화라는 치명적인 부작용을 동반했습니다. 즉 동일한 코드로 작성된 웹페이지나 웹 앱임에도 불구하고 다양한 브라우저 환경에 호환되지 않아 각 환경별로 대응이 필요한 상태가 되었습니다.

브라우저에 따라 전혀 다른 화면이나 동작결과가 발생하여 사용자는 브라우저의 종류와 상관없이 동일한 경험을 얻을 것이라 생각하는데 이는 민감할 수밖에 없는 문제로 이어지고 있습니다.

<주요 웹 브라우저>



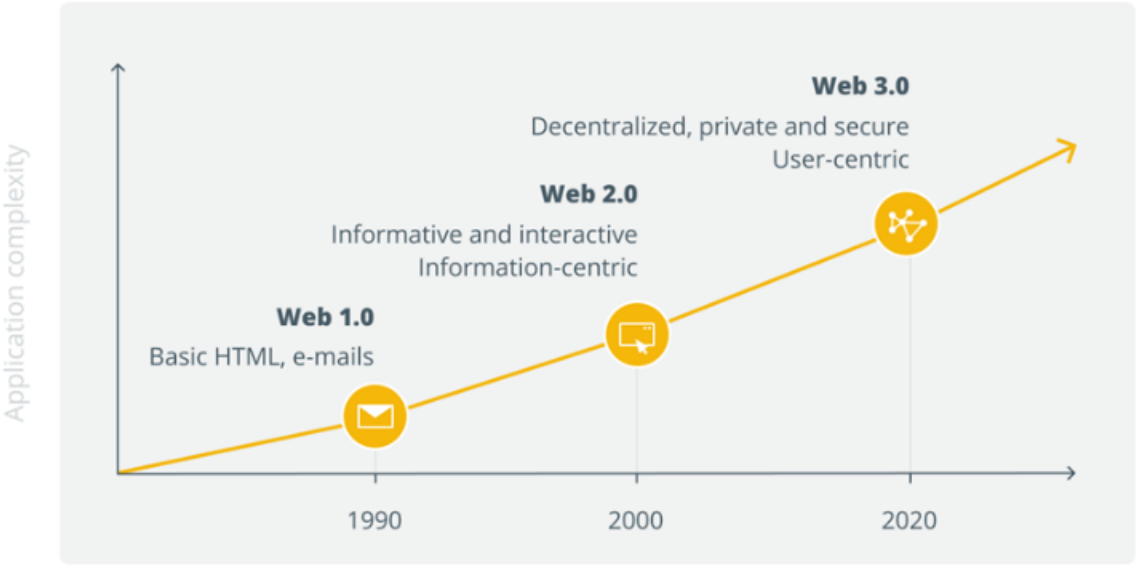
<웹 브라우저 타임라인>

파편화 해결을 위해 여러 개발사들은 꾸준히 웹 표준화를 위해 노력해왔습니다.
대표적인 웹 표준인 HTML・CSS・ECMAScript는 지속적으로 개정되었고 각 웹 브라우저 개발사들은 이를 준수하고 있습니다. 그러나 웹 표준이 만들어지는 과정에서 방향성에 대한 의견 차이로 인해 이 표준이 분리되는 상황이 나타나기도 했습니다. 결국 웹 표준을 준수하도록 작성된 코드가 브라우저 간 완벽하게 호환되지 않는 파편화 현상은 여전히 나타나고 있습니다.

2020년 1월 31일 부로 윈도우7과 함께 인터넷 익스플로러10의 공식 기술 지원이 종료되었습니다. 또한 인터넷 익스플로러11도 윈도우 보증기간 종료와 함께 기술지원이 종료될 예정입니다. 마이크로소프트는 Edge 브라우저를 공식 브라우저로 지정하고 있지만 타 브라우저에 비해 이용이 많이 불편한 것이 현실입니다.

1.2 MPando Browser 와 Web 3.0

MPando Browser는 컴퓨터가 시맨틱 웹(semantic web) 기술을 이용하여 웹 페이지에 담긴 내용을 이해하고 개인 맞춤형 정보를 제공할 수 있는 지능형 웹 기술인 Web3.0 기반으로 개별 사용자에게 맞춤화된 서비스를 제공하는 브라우저입니다.



<History of the Internet>

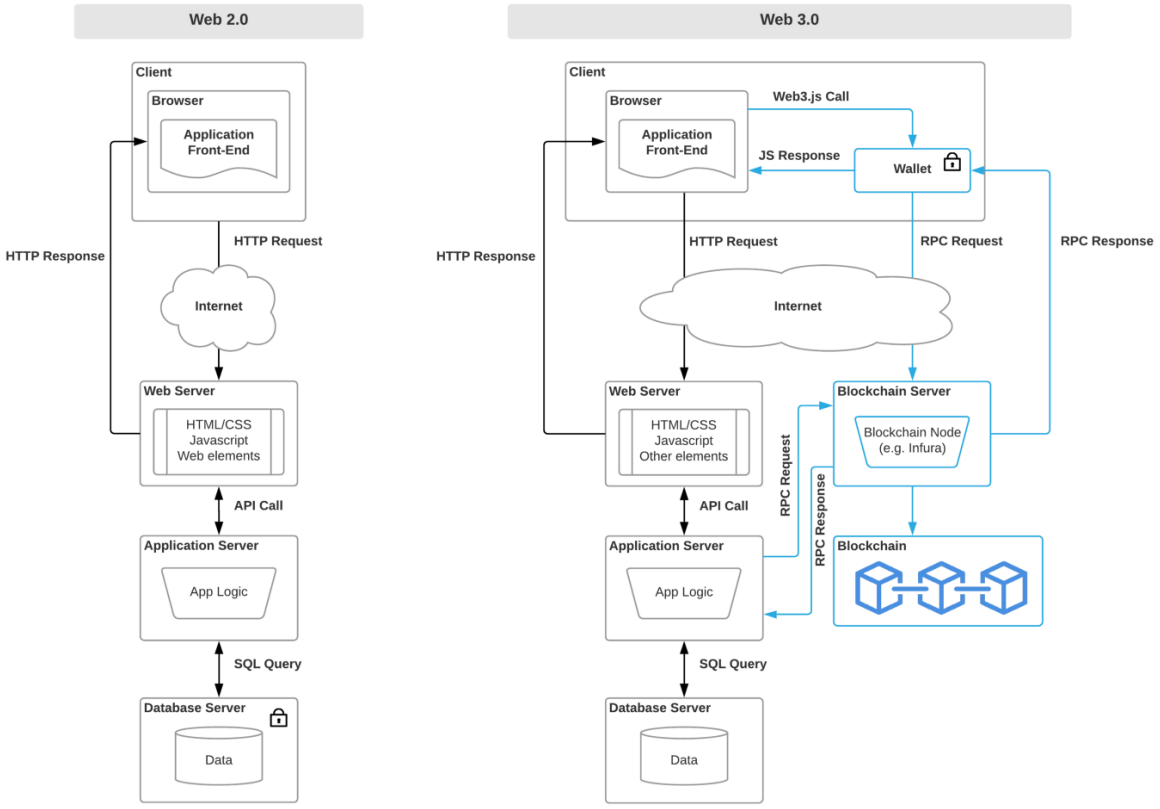
Web 2.0기술은 파편화되고 방대해진 정보를 서로 연결하지 못하는 단점이 있었으며 Facebook, Twitter, LinkedIn 등의 SNS 사이트와 카카오톡, 라인, Wechat 등의 메신저 서비스가 대표합니다.

팀 버너스 리(Tim Berners-Lee)는 웹에 존재하는 모든 데이터에 의미를 부여해 컴퓨터가 이해할 수 있는 지능화된 웹을 만들고, 사람이 관여하지 않아도 컴퓨터가 신속하게 자동으로 처리할 수 있는 인터넷 환경을 구현하기 위해 시맨틱 웹 기술을 만들었습니다.

시맨틱 웹 기술을 기반으로 온톨로지(Ontology)와 메타데이터(Metadata) 기술이 발전했고 해당 기술을 기반으로 Web2.0 기술의 단점을 보완하는 Web3.0 시대가 열리게 되었습니다.

Web3.0은 블록체인(BlockChain) 기술이 지닌 특성을 이용해 구축되는 새로운 생태계입니다. 약 3,000개가 넘는 분산형 DApp (Decentralized Application)으로 구성되어 있습니다.

DApp은 탈중앙집권의 애플리케이션으로 중앙 컨트롤의 주체가 없으며 네트워크를 유지하는 역할만 하며 관리하는 권한은 가지고 있지 않습니다. 따라서 사용자는 자신이 데이터를 소유하고, 데이터를 공유할 사람을 선택함에 따라 디지털 프로필에서 재정적 보상을 얻을 수 있게 해줍니다.



<Web2.0과 Web3.0 애플리케이션의 아키텍처>

MPando Browser는 Web3.0 기반으로 개발되어 탈중앙화가 주는 이점을 가지고 있습니다.

중개인은 사라지게 되며 이더리움(Ethereum)과 같은 블록체인은 규칙을 위반할 수 없으며 데이터는 완벽하게 암호화되기 때문에 제3자가 존재하지 않아도 믿고 거래할 수 있는 플랫폼을 제공합니다.

정부 또는 기관들도 사용자의 데이터를 지배할 권리를 갖지 못하며, 개인이 다른 이의 신원정보 또한 지배할 수 없습니다. 이는 정부나 기업의 검열 위험을 줄이고, 서비스 거부 공격(DoS, Denial-of-Service attack 시스템을 악의적으로 공격해 해당 시스템의 리소스를 부족하게 하여 네트워크에 접근하지 못하게 방해하는 공격)의 영향을 덜 받게 됩니다.

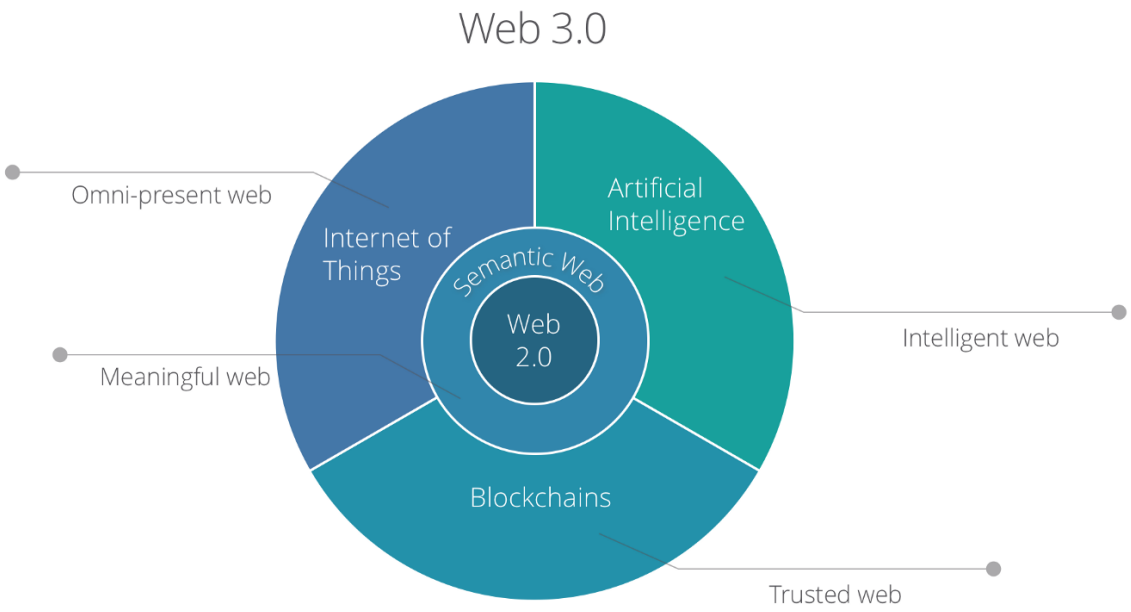
사용자는 데이터에 대한 100%의 권한을 되찾게 되며 그 데이터는 암호화되어 보호됩니다. 타 기업이 개인의 선호 수입, 식단, 관심사 등의 메타데이터들을 마음대로 사용하지 못합니다. 데이터가 탈중앙화되고 분산되어 저장되기 때문에 해커는 네트워크 전체를 해킹해야 하므로 해킹 및 데이터 유출 또한 급격히 감소하게 될 것입니다.

Web3.0 기술 기반 하에서는 어플리케이션의 커스터마이즈(Customize)가 용이하고 스마트폰, 자동차, TV, 전자레인지, 스마트 센서 등 기기에 상관없이 실행이 가능합니다. 인터넷에 연결되어 있는 결과물들이 점차 증가함에 따라, 보다 큰 일련의 데이터는 분석할 수 있는 더 많은 정보와 함께 알고리즘을 제공하게 됩니다. 이에 따라 개별 사용자들의 특정한 요구를 충족시키는 정확한 정보를 제공하는데 도움을 주어 보다 효율적인 브라우징이 가능해집니다.

과거에 검색 엔진을 통해 원하는 결과값을 얻는 것은 꽤나 어려운 일이었습니다. 그러나 몇 년 동안 이는 검색 맥락과 메타데이터를 기반 삼아 의미상으로 연관된 결과를 전보다 더욱 잘 찾아내게 되었습니다. 이는 자신이 원하는 정확한 정보를 누구나 상대적으로 쉽게 찾을 수 있게 도와주는 보다 편리한 웹 브라우징 경험으로 이어지게 됩니다.

효율적인 알고리즘(Algorithm)을 이용하면, 인공지능(AI, Artificial Intelligence)을 통해 조작된 검색 결과들을 필터링 할 수 있습니다. 그리고 누구나 주소를 생성하고 네트워크와 상호 작용하는 것이 가능해지며, 부(Wealth)와 디지털 자산은 전 세계를 넘나들며 효율적이며 빠르고 안전하게 전송할 수 있게 됩니다. 또한 중단 없이 서비스를 제공하는 것이 가능합니다. 따라서 계정 일시 중지 및 서비스 지연이 큰 폭으로 감소할 것입니다.

단일 장애점(SPOF, Single Point of Failure)이 존재하지 않기 때문에, 서비스 장애가 최소화됩니다. 데이터는 분산된 노드에 중복으로 저장되기 때문에 복수의 백업을 확보하게 되며, 이로 인해 서버 오류나 서버 압수 등에 대응할 수 있습니다.



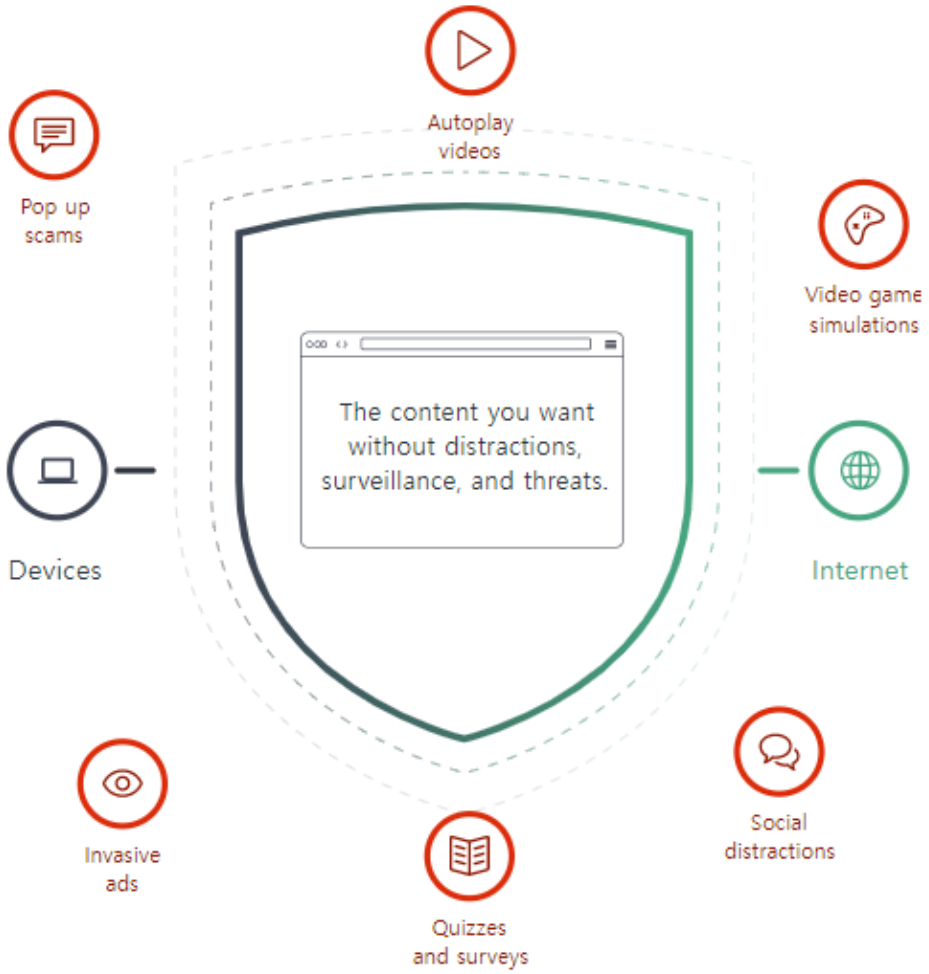
<AI, IoT (Internet of Things, 사물인터넷) 및 블록체인의 융합>

Web3.0 기술은 광고와 마케팅 분야에서도 많은 부분이 개선됩니다.
원치 않은 방대한 온라인 광고를 좋아하는 사람은 없지만, 해당 광고가 누군가의 관심과 필요에 적합하다면, 이는 불편한 내용이 아닌 유용한 정보에 해당됩니다. 더욱 진화된 인공지능 시스템을 활용해 광고를 개선하며, 소비자 데이터를 기반으로 특정한 대상을 표적화합니다.

MPando Browser는 더욱 나은 고객 서비스를 지원합니다.
웹사이트와 웹 애플리케이션에서 고객 서비스는 원활한 사용자의 경험의 핵심이지만 막대한 비용 때문에, 성공적인 많은 웹 서비스들이 이에 맞춰 고객 서비스 규모를 확장하지 못합니다. 그러나 MPando Browser는 여러 고객과 동시에 커뮤니케이션 할 수 있는 스마트한 채팅 봇을 활용함으로써, 사용자들은 서비스 에이전트보다 더 우수한 서비스를 누릴 수 있게 됩니다.

2.1 SmartBlock

개인 브라우징 및 향상된 Tracking Protection에서 MPando Browser는 추적기로부터 웹 브라우징 활동을 보호하기 위해 많은 노력을 기울입니다. 그 일환으로 내장된 콘텐츠 차단 기능은 제3자 스크립트, 이미지 및 기타 콘텐츠가 Disconnect에서 보고한 사이트 간 추적 회사에서 로드되는 것을 자동으로 차단합니다.
이러한 유형의 공격적인 차단은 때때로 이미지 누락 또는 성능 저하와 같은 작은 불편을 초래할 수 있습니다. 매우 드문 상황으로 기능 오작동이나 빈 페이지가 발생할 수 있습니다.



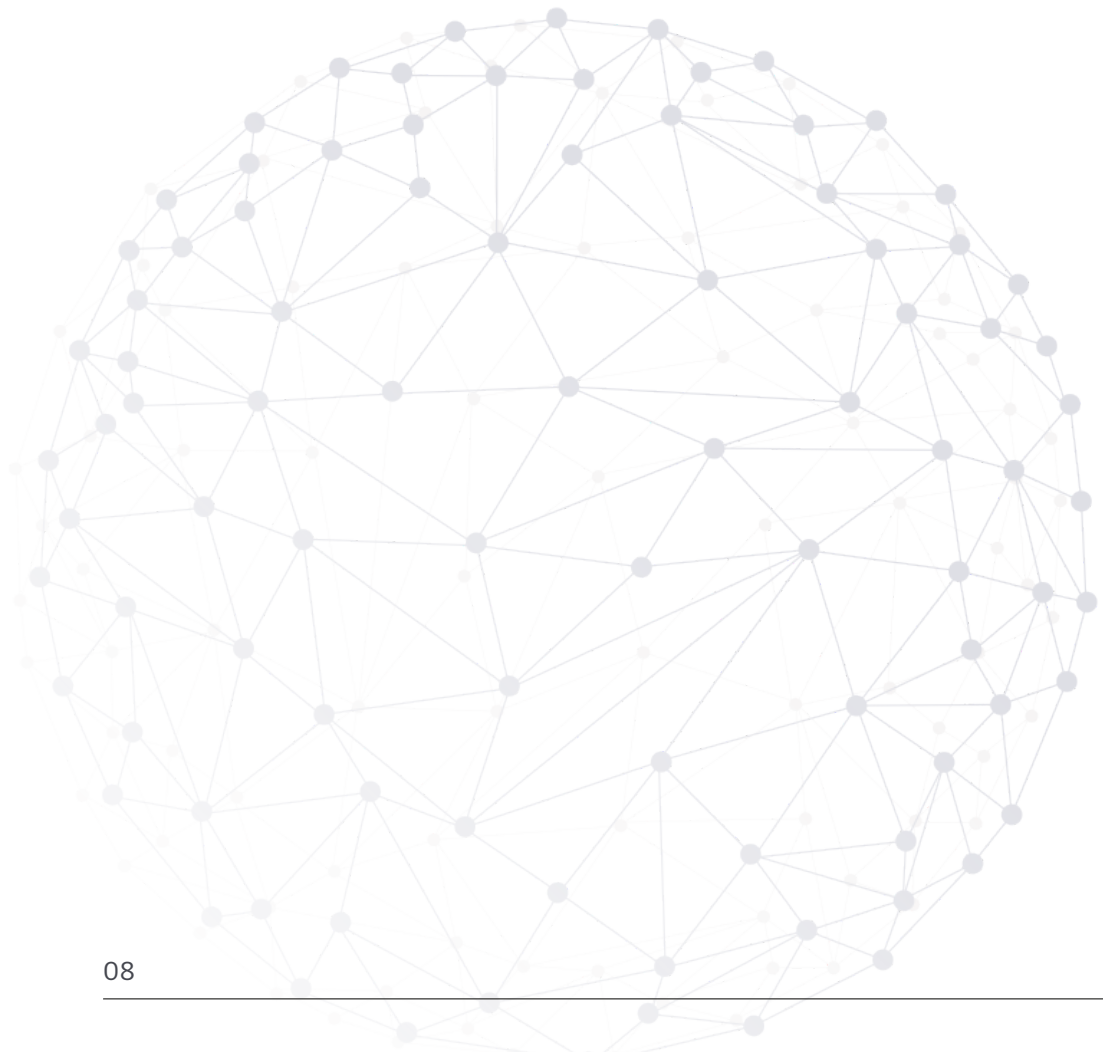
<Disconnect Tracking Protection>

이를 보완하기 위해 우리는 웹사이트가 제대로 작동하는지 확인하기 위해 원래 리소스처럼 충분히 작동하는 차단된 리소스에 대한 로컬의 개인 정보 보호 대안을 지능적으로 로드하는 메커니즘(Mechanism)인 SmartBlock을 개발했습니다.

SmartBlock은 추적 보호(Tracking Protections) 기능으로 오작동이나 빈 페이지가 발생할 경우 사용자의 개인 정보를 침해하지 않고 지능적으로 수정합니다. 또한 차단된 타사의 추적 스크립트의 로컬 대역을 제공하여 수정 작업을 진행합니다.
이러한 독립 실행형 스크립트는 웹 사이트가 제대로 작동하는지 확인할 수 있는 원본의 스크립트와 동일하게 동작합니다. 이런 기능을 사용하여 기존 스크립트에 의존하는 손상된 사이트를 그대로 로드할 수 있습니다.

SmartBlock의 세 번째 버전에서 널리 사용되는 Google Analytic 스크립트를 대체하기 위한 지원이 크게 향상되었으며 Optimizely, Criteo, Amazon TAM 및 다양한 Google 광고 스크립트와 같은 인기 서비스에 대한 지원이 추가되었습니다.

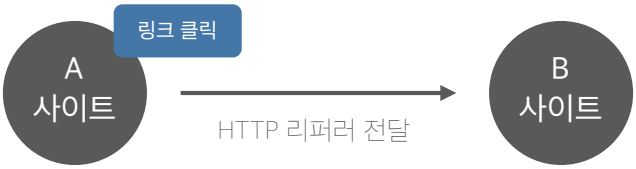
SmartBlock의 이러한 대체 기능은 판도 브라우저에 번들로 제공되며, 추적기의 타사 컨텐츠가 전혀 로드되지 않으므로 어떤 방식으로도 사용자를 추적할 수 없습니다.



2.2 HTTP Referrer 보호

HTTP Referrer 헤더는 웹 브라우저를 이용하여 웹을 서핑할 때, 하이퍼링크를 통해서 각각의 사이트로 방문 시 남는 흔적을 말합니다.

현재 요청을 보낸 페이지의 절대 혹은 부분 주소를 포함하게 되며, 링크를 타고 들어온 경우 해당 링크를 포함하고 있는 페이지의 주소가, 다른 도메인에 리소스 요청을 보내는 경우라면 해당 리소스를 사용하는 페이지의 주소가 이 헤더에 포함됩니다.
웹 사이트에서 분석, 로깅 및 캐시 최적화를 위해 자주 사용됩니다. 그러나 여기서 문제가 발생합니다.
브라우저가 이전 사이트의 전체 URL을 보내는 경우 URL을 통해 민감한 사용자 데이터가 노출될 수 있습니다. 일부 사이트는 Referrer 헤더에 언급되는 것을 피하고 싶을 수 있습니다.



Referrer 정책은 이 문제를 해결하기 위해 도입되었습니다.
웹 사이트에서 Referrer 헤더의 값을 제어할 수 있으므로 사용자에 대해 보다 강력한 개인정보 보호를 설정할 수 있습니다.

MPando Browser는 한 단계 더 나아가 새로운 기본 Referer 정책을 Strict-origin-when-cross-origin으로 설정하여 다른 웹사이트와 공유할 때 더욱 강력하게 개인정보를 보호합니다.
Cross-origin 요청인 경우에는 Referrer에 origin값만 전달하기 때문입니다. 따라서 URL path, query string에 포함된 개인정보가 유출될 가능성을 막아줍니다.

Version 93의 출시와 함께 MPando Browser는 'no-referrer-when-downgrade', 'origin-when-cross-origin' 및 ' unsafe-URL'과 같은 사이트 간 요청에 대한 비교적 덜 제한적인 Referer정책을 무시합니다. 그리하여 개인정보가 유출될 가능성을 막아줍니다.

Referer 정책이 설정되어 있지 않은 경우, MPando Browser의 기존 정책이 적용됩니다.
다시 말하면, MPando Browser는 웹사이트의 설정에 관계없이 항상 교차 사이트 요청에 대한 HTTP Referer를 트리밍(Trimming) 합니다.

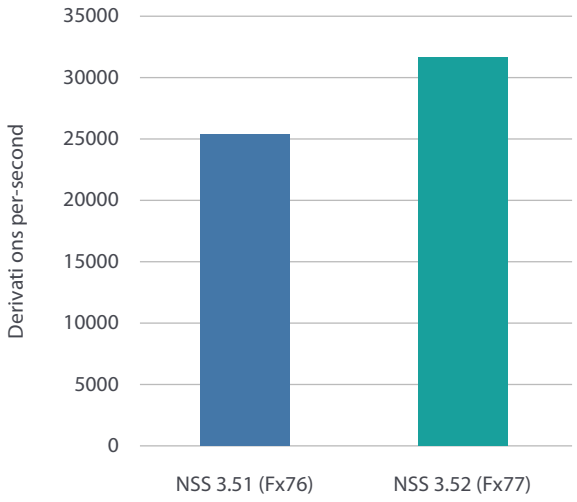
동일한 사이트 요청의 경우 웹사이트는 물론 전체 Referer URL을 보낼 수 있습니다.

2.3 국제인터넷 표준화기구(IETF)의 표준화 인증을 통해 검증된 암호화 기술

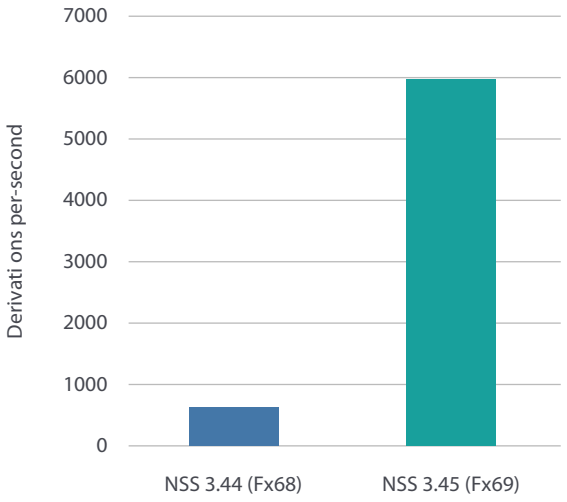
핵심 설정을 위해 최근 기존 Curve25519의 32bit 구현을 Fiat-Crypto 프로젝트의 구현으로 교체하였습니다.
이 구현의 임의 정밀도 산술 함수는 기능적으로 올바른 것으로 입증되었으며 기존 코드에 비해 10배 향상되었습니다.

MPando Browser는 64비트를 구현함에 있어 새로운 HACL* 코드로 업데이트하여 이전 버전 대비 ~27% 속도 향상을 이루었습니다. MPando Browser는 최근에 이 업데이트를 Windows에도 제공하였습니다.

이와 같은 개선사항은 매우 중요합니다. Telemetry는 Curve25519가 MPando Browser의 ECDH(E) 키 설정에 가장 널리 사용되는 타원 곡선형태를 이루며 모바일 장치와 접목 시 처리량 증가 대비 에너지 소비가 감소하며 이는 모바일 장치에서 특히 중요한 요소로 작용됩니다.



<64비트 curve25519(HACL 포함)>



<Fiat-Crypto 가 포함된 32 비트 Curve25519>

Curve25519의 산술적 성질을 살펴보면 다음과 같습니다 .

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

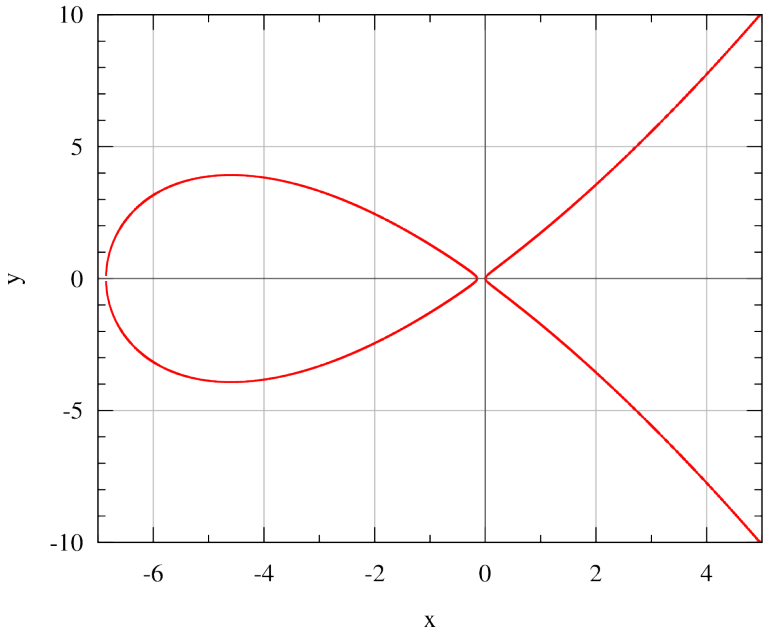
사용된 곡선은 소수 $2^{255} - 19$ 로 정의된 소수 영역 위의 몽고메리 곡선입니다.
그리고 기준점으로 $x = 9$를 사용합니다. 이 기준점은 소수를 순서로 하는 순환 하위 그룹을 생성합니다. 이 하위 그룹은 아래 소수를 나타냅니다.

$$2^{252} + 27742317777372353535851937790883648493$$

이 하위 그룹의 Co-factor 는 8 이며 이는 하위그룹의 구성 요소의 수가 1/8 임을 의미합니다.
몽고메리 곡선은 (필드 K) 다음의 방정식으로 정의됩니다.

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

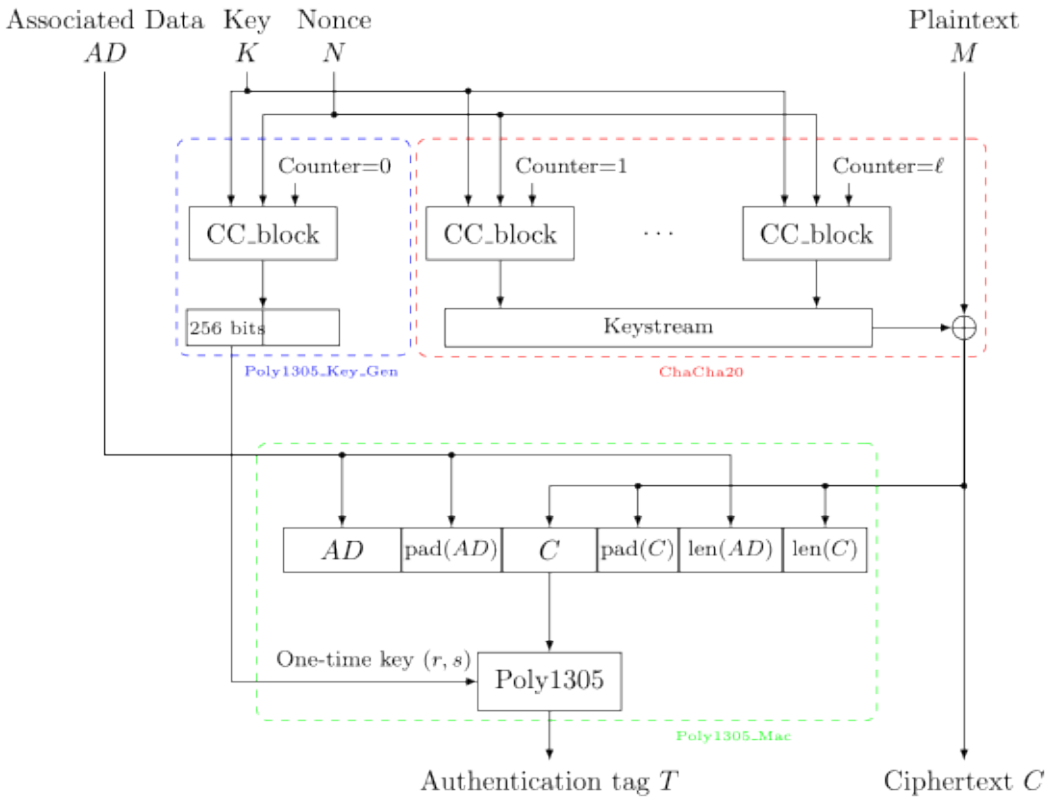
특정 $A, B \in K$ 이고 동시에 $B(A^2 - 4) \neq 0$



<curve25519 몽고메리 곡선>

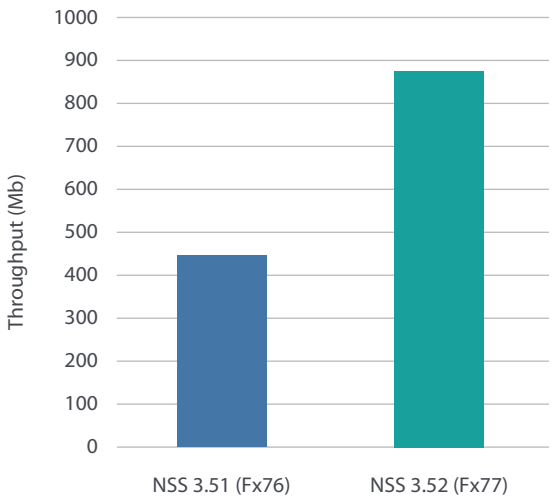
MPando Browser는 암호화 및 암호 해독을 위해서 ChaCha20-Poly1305의 성능을 개선했습니다.

ChaCha20-Poly1305는 ChaCha20 스트림 암호와 Poly1305 메시지 인증 코드를 결합한 AEAD(Authenticated Encryption with Additional Data) 알고리즘입니다.



ChaCha20-Poly1305 알고리즘은 일반적으로 CPU에 하드웨어 가속 기능이 없는 시스템에서 널리 사용되는 AES-GCM 알고리즘보다 더 나은 성능을 제공합니다.

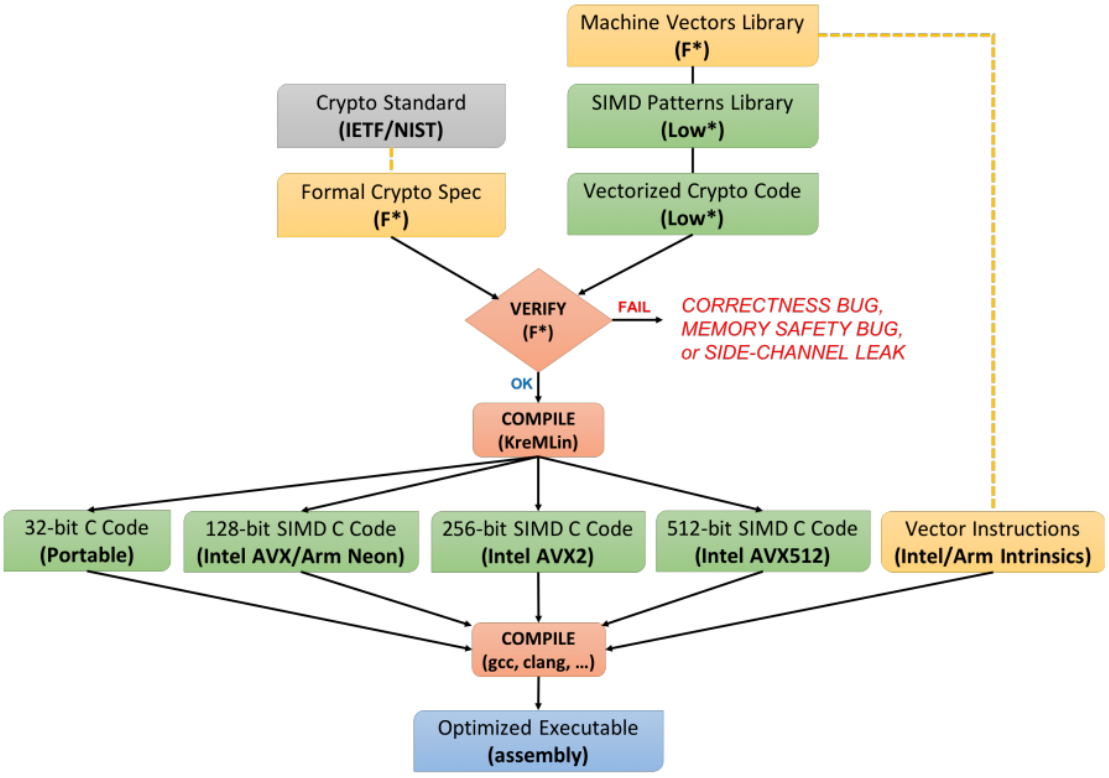
128비트 및 256비트 정수 산술(x86-64 CPU에 설정된 AVX2 명령어 사용)을 통한 벡터화를 활용하여 처리량이 두 배로 증가했습니다. 이러한 기능을 사용할 수 없는 경우 NSS는 AVX 또는 스칼라 구현으로 대체되며 둘 다 더욱 최적화됩니다.



<HACL* 및 AVX2 가 포함된 ChaCha20 Poly1305>

HACL* 프로젝트는 스칼라 및 벡터화 된 변형 모두에 대해 검증된 기본 요소 작성의 효율성을 개선하기 위하여 새로운 기술과 라이브러리를 도입했습니다.

이를 통해 공격적인 코드 공유가 가능하고 다양한 플랫폼에서 검증 노력이 줄어듭니다.



<HACL Programing and Verification Workflow>

2.4 Private 브라우징 모드

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

우리가 정기적으로 온라인에 접속할 때 이용하는 브라우저에서 높은 수준의 데이터 보호 및 개인 정보 보호를 기대하고 신뢰한다는 것은 불가능한 일이 아닙니다.

이는 MPando Browser에 Private 브라우징을 이용하여 방문 기록, 검색 기록, 서식 기록 등 로컬에 남는 흔적들을 자동으로 삭제해주기 때문입니다.

또한 사용자에게 필요한 북마크나 다운로드 등의 흔적은 안전하게 보호됩니다.

2.5 MPando Browser 유용성

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	✓	—	✓	—	✓	—	—

일반적으로 브라우저의 백그라운드에서 발생하는 개인 정보 보호 외에도 잘 만들어진 브라우저의 또 다른 핵심 요소는 실제 사용자 인터페이스(Interface)와 기능입니다.

MPando Browser는 자동 재생 차단, 텍스트 음성 변환, 브라우저 내 스크린 샷 도구 제공 등 크롬, 사파리, 오페라, 익스플로러에서 지원하지 않는 기능들을 모두 제공하며 처리 속도 또한 더욱 빠르고 안전합니다.

2.6 MPando Browser 휴대성

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

인터넷 사용 유저가 전세계 약 50억 명에 이르는 시대에 웹 브라우저를 선택하며 휴대성은 가장 중요한 요소입니다. 한 가지 지적할 사항은 모든 브라우저가 모든 운영 체제를 지원하지 않는다는 것입니다. 즉 일부 웹 브라우저는 운영체제에 따라 이용이 불가합니다.

Firefox, Chrome, Edge, Brave 및 Opera는 모든 주요 시스템에서 작동하고 설치 또한 용이한 반면 Internet Explorer 및 Safari의 경우 Microsoft 및 Apple 자체 시스템에서만 작동합니다. Apple의 모바일 기기에는 Safari 브라우저가 기본으로 사전 설치되어 있으며 대부분의 Android 기기에는 제조업체에서 해당 기기에 맞게 수정된 웹 브라우저가 사전 설치되어 제공되고 있습니다.

그러나 MPando Browser는 Firefox, Chrome, Brave, Edge, Opera처럼 모든 운영체제 및 기기에서 쉽게 설치하고 이용할 수 있습니다.

MPando Browser는 대부분의 웹 브라우저가 지원하는 데스크톱과 모바일 장치 간의 동기화를 지원합니다. 이용 중인 모든 기기에서 MPando Browser에 로그인하고 비밀번호, 인터넷 사용기록, 책갈피 및 설정과 같은 항목을 동기화하여 사용할 수 있습니다.

2.7 사용자의 편의성을 높여주는 다양한 애드온 제공

MPando Browser는 다양한 애드온을 손쉽게 구성/설치할 수 있으며, 사용자 환경에 맞게 커스터마이징 된 환경을 제공합니다. MPando Browser에서 제공하는 애드온 기능을 통해 더욱 다양한 판도만의 서비스를 이용할 수 있습니다.