Onther Inc.

Smart Contract Project

정다운
tyrannojung@korea.ac.kr
23/12/21

https://onther.io/onther-tech

Authentication in Web 2.0 and Web 3.0

Onther Inc.

Evolution of Traditional Web 2.0 Authentication Methods

Web 1.0: Read-Only → No Authentication Required

Web 2.0: Read-Write → Web & Server Interaction → Authentication Required (**Server Storage**)

→ Gradually Evolving Towards Self-Storage of Data

Web 3.0 : Read-Write-Own → Web & Blockchain Interaction → Self-Ownership (Decentralization)

Onther Inc.

Evolution of Traditional Web 2.0 Authentication Methods

Web 1.0: Read-Only → No Authentication Required

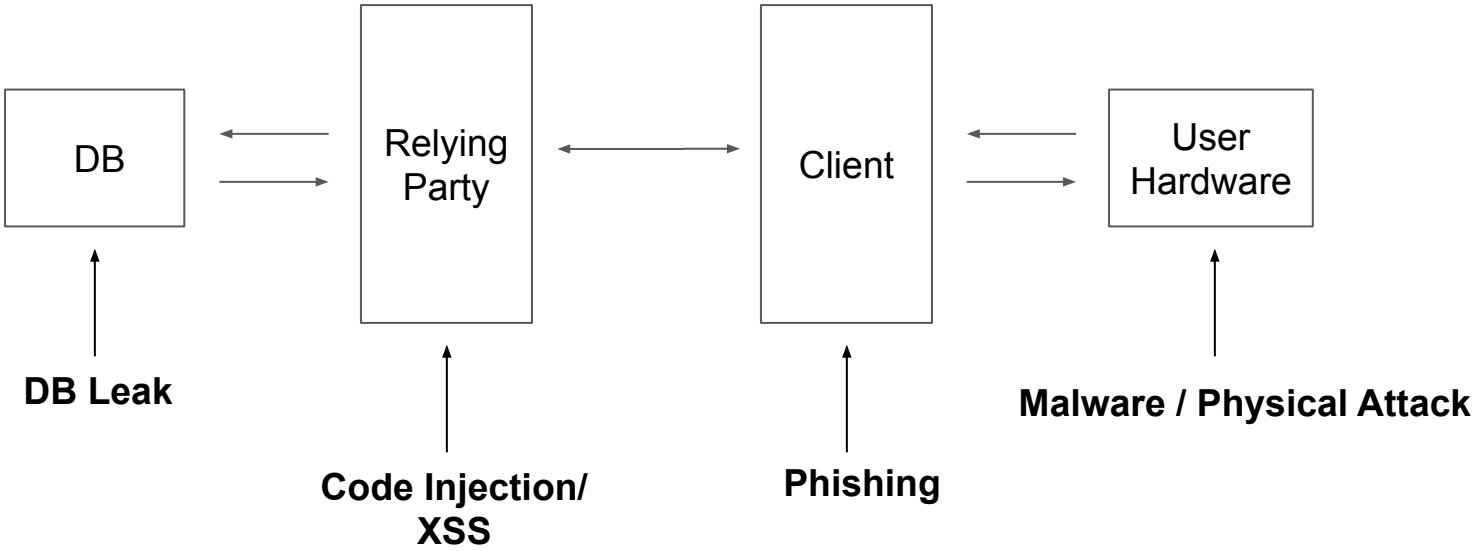
Web 2.0: Read-Write → Web & Server Interaction → Authentication Required **(Server Storage)**

→ Gradually Evolving Towards Self-Storage of Data

Web 3.0 : Read-Write-Own → Web & Blockchain Interaction → Self-Ownership (Decentralization)

Onther Inc.

Evolution of Traditional Web 2.0 Authentication Methods



Web2.0 - Attack Scenarios

Onther Inc.

Evolution of Traditional Web 2.0 Authentication Methods

Client to server model authentication

- Online isolated identity management(Fig. 1)
- Federated isolated identity management(Fig. 2)
- Local device identity management
- Fast Identity Online(FIDO)

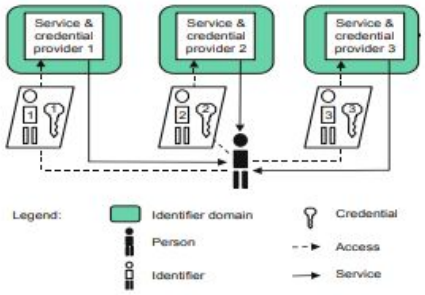


Fig. 1. Isolated Online Identity Management

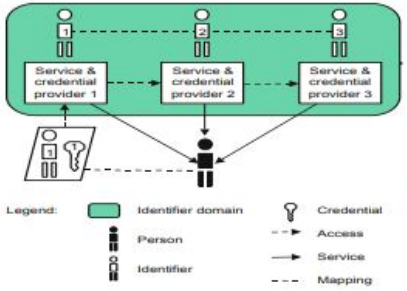


Fig. 2. Federated Online Identity Management

Onther Inc.

Evolution of Traditional Web 2.0 Authentication Methods

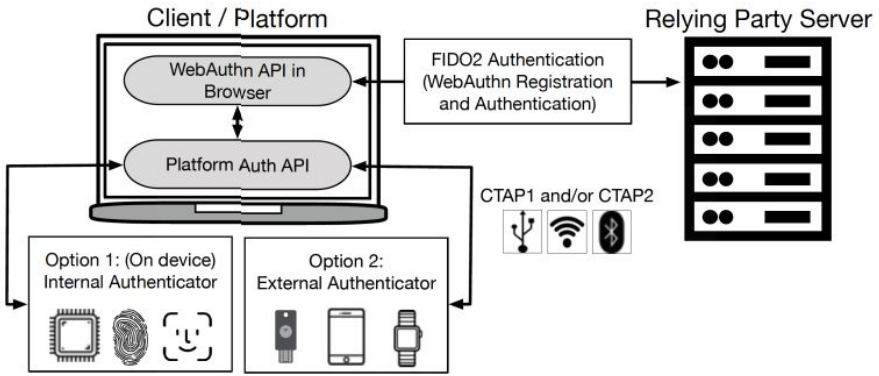


Figure 1: FIDO2 authentication with WebAuthn and CTAP2. This diagram is taken from Lyastani et al. [26].

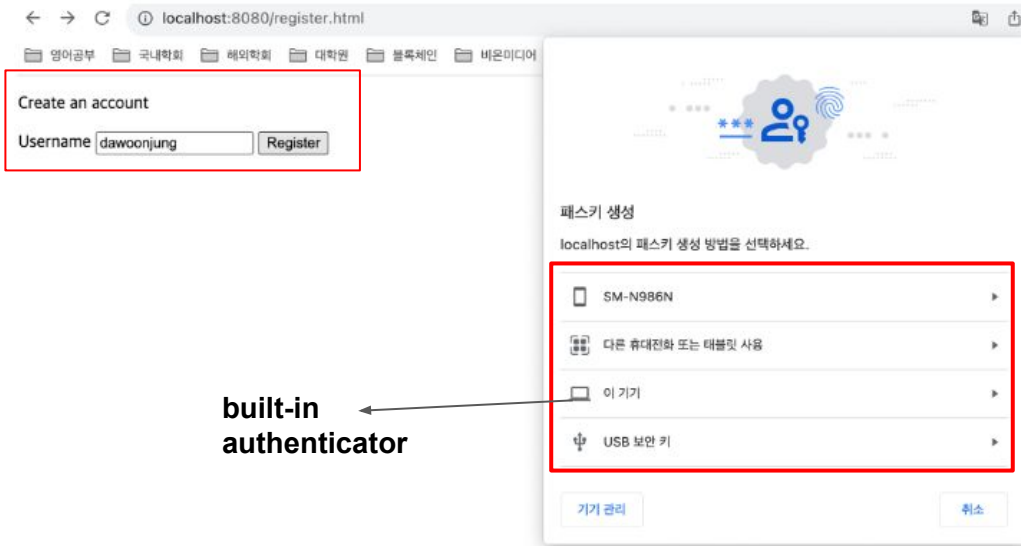
- The FIDO2 protocol is a globally adopted standard for passwordless authentication, built on alliances among major players in the online authentication space. It brings together over 40 leading companies in the online authentication field, including Amazon, Apple, Google, Intel, Microsoft, RSA, VISA, and Yubico.
-
- It communicates with devices using the WebAuthn API supported by JavaScript in web browsers.
- It has commonly been used in 2FA (Two-Factor Authentication) setups.

Onther Inc.

Evolution of Traditional Web 2.0 Authentication Methods

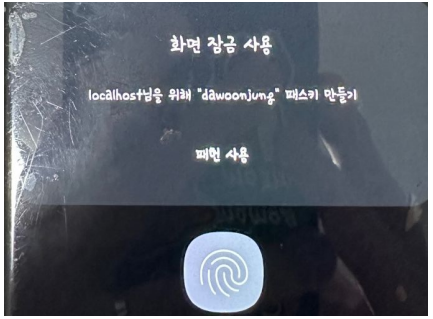
1. web application

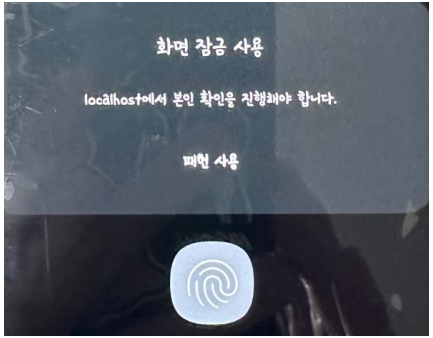
2. web browser



built-in authenticator

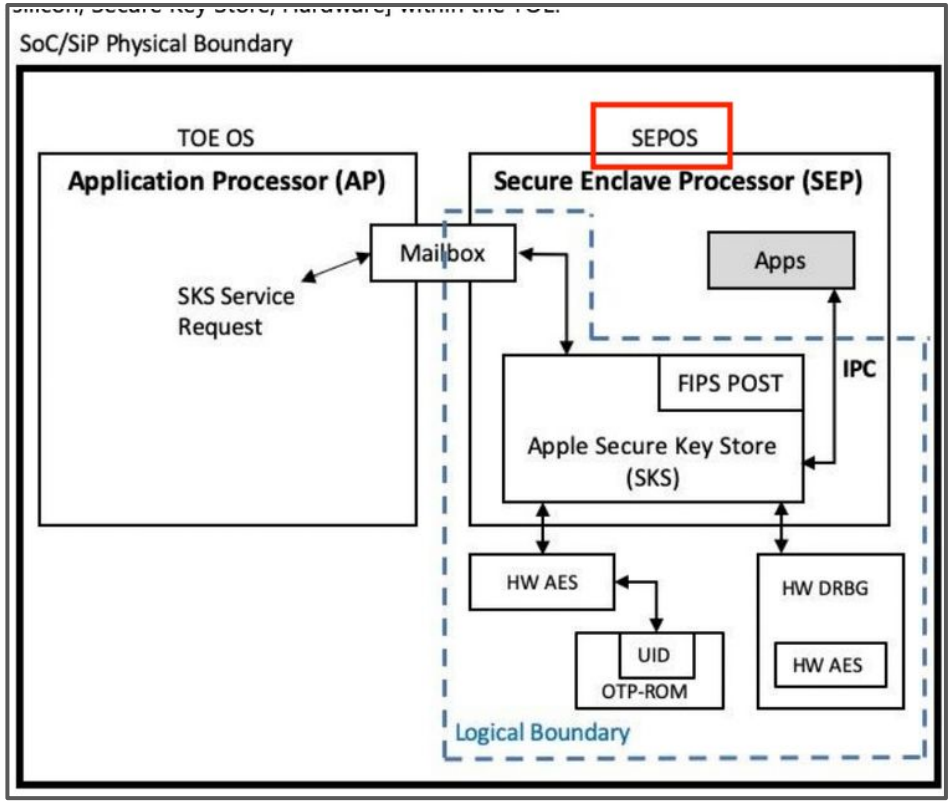
3. external authenticator





Onther Inc.

Evolution of Traditional Web 2.0 Authentication Methods



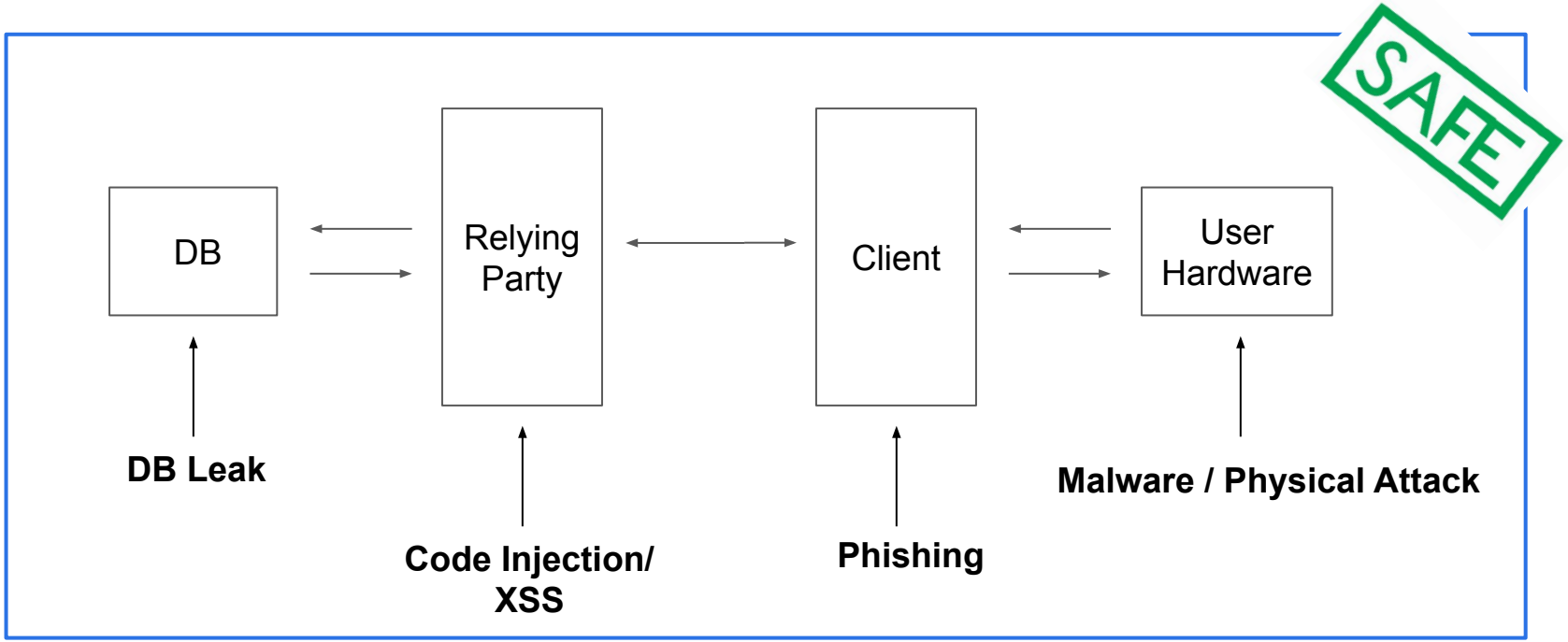
Secure Enclave (iOS)

- Isolated area from the central processor
  - Own operating system, SEPOS
- Securely stores and manages biometric data like Touch ID and Face ID
- 4MB of storage space
- Supported Cryptographic Algorithms:
  - ECDSA (P-256, P-384), RSA, EdDSA, HMAC, etc.
  - Does not support the secp256k1 algorithm

- In Android, ARM TrustZone (TEE) serves a similar function.

Onther Inc.

Evolution of Traditional Web 2.0 Authentication Methods



→ *Using FIDO, our application has become secure against various threats.*

Onther Inc.

Partial Summary

1. FIDO, developed in WEB 2.0 by a consortium of major corporations including Google and Amazon, is an authentication standard that is secure against various security threats.

2. It features a secure storage operating on an independent processor within the device, supporting asymmetric key algorithms (e.g., elliptic curve, P-256).

3. A standard protocol (CTAP) exists for communication between external (including internal) devices and browsers, and is supported by most browsers.

4. Adopted as a W3C standard, it enables the direct use of JavaScript APIs in web applications without the need for browser plugin installations.

Promoting Mass Adoption of Web 3.0 with ERC 4337

Onther Inc.

Onther Inc.

Web 3.0 Wallet Authentication: Challenges and Security Concerns

In Web 3.0, authentication is primarily through wallets.

Challenges:

1. Popularized wallets have security vulnerabilities.
2. To use blockchain wallets, a high learning curve exists – a barrier to widespread blockchain adoption.

Onther Inc.

Problem 1: Security Issues

Phishing Attack

거래소 이어 유명인도 당했다… 연일 코인 해킹에 '시끌'

정다운 기자 (tyrannojung@bonmedia.kr)

글씨크기

NBA 댈러스 구단주, 지갑 해킹으로 약 10억 원 피해
앞서 거래소 '코인엑스' 핫월렛 해킹도… 북한 소행 추정
해킹 방식 다양화… 민관 협력, 표준화된 대응책 필요

인기기사

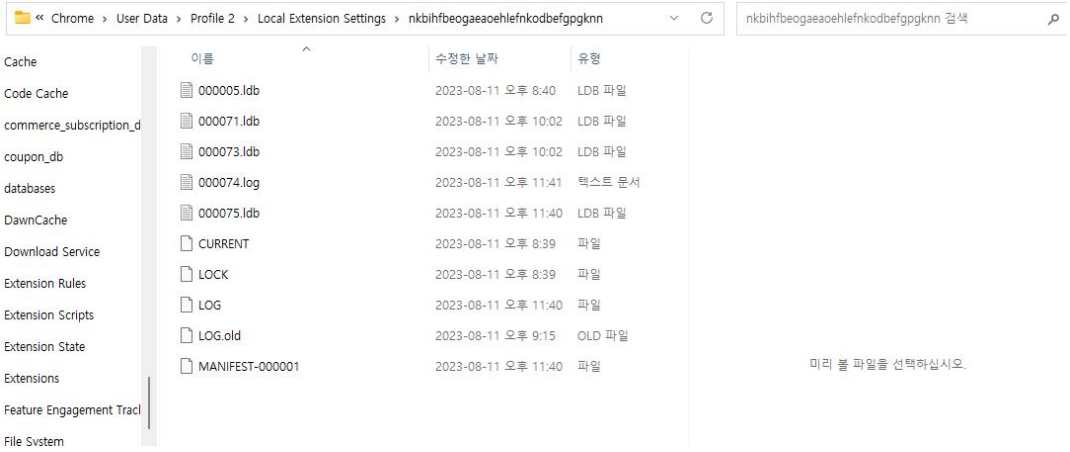
1 '김치 프리미엄' 노린 16조 외화송금… 은행권 중징계

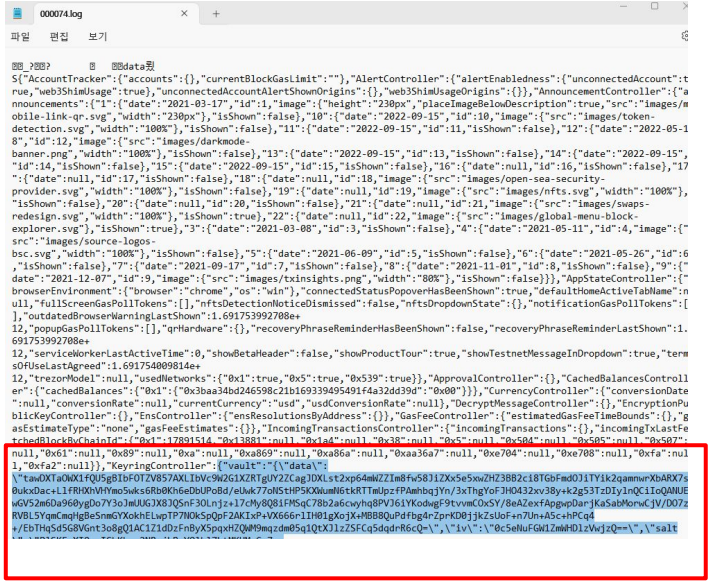
큐반은 해킹의 원인으로 악성 메타마스크 확장 프로그램을 지목했다. 그는 금융 전문 미디어 디엘뉴스와의 인터뷰에서 "나는 메타마스크 악성 버전을 다운 받아 해킹 당했다고 확신한다"며 "몇 달 만에 처음으로 메타마스크를 사용했고 해커는 내가 비밀번호를 푸는 순간을 기다렸을 것"이라고 말했다. 실제로 메타마스크와 같은 핫월렛 지갑은 온라인으로 연결되어 있다는 특성 때문에 악성 프로그램을 다운 받을 시 이번 도난 사건과 같은 해킹에 취약하다.

Onther Inc.

Problem 1: Security Issues

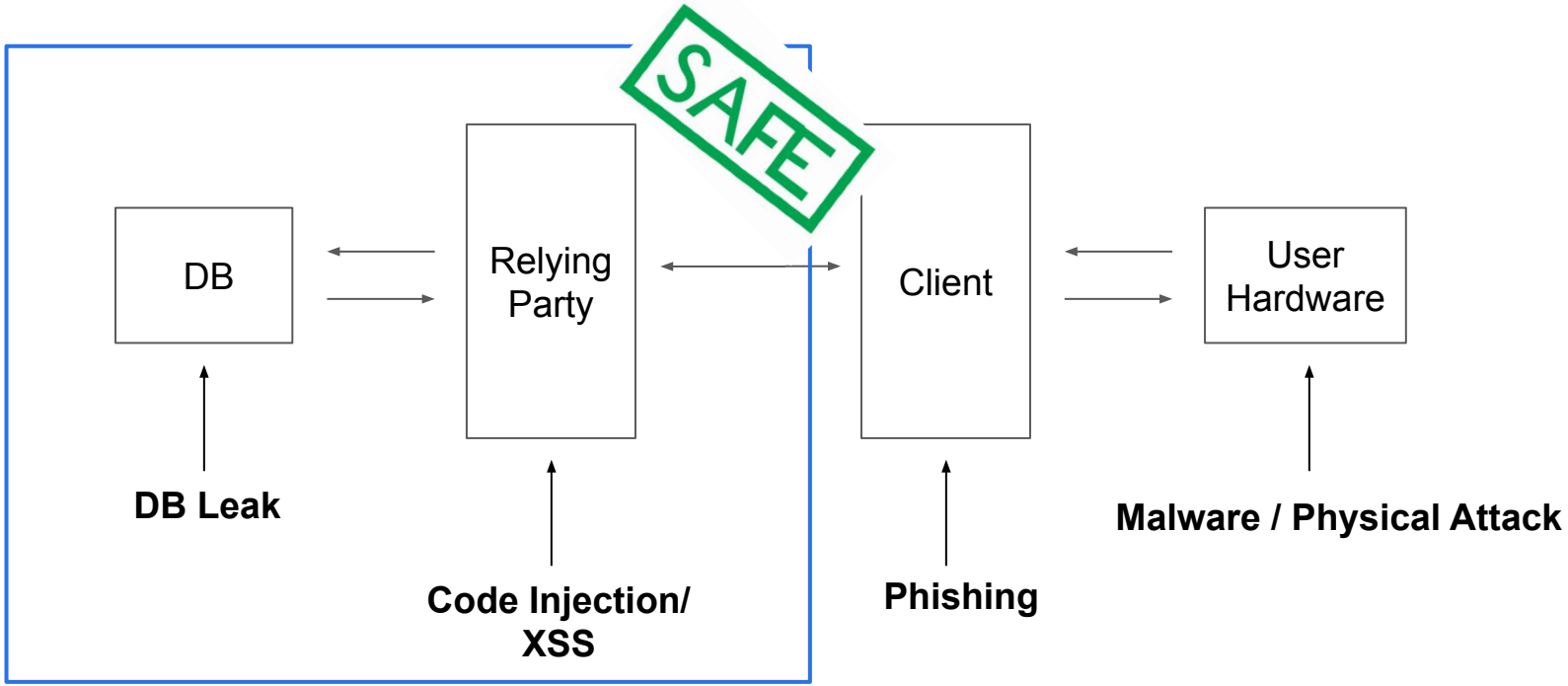
Malware Attack





Onther Inc.

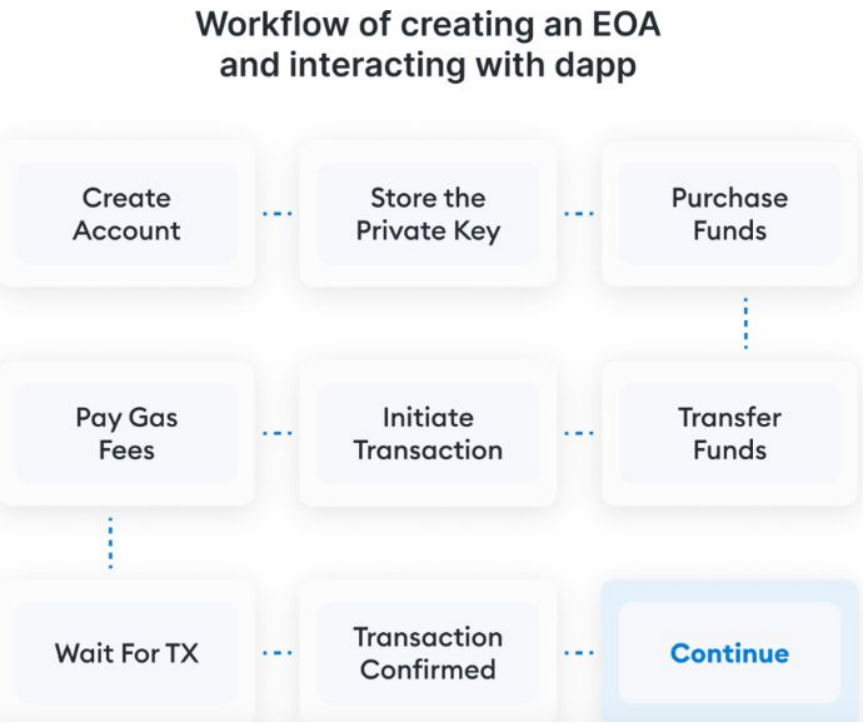
Problem 1: Security Issues



→ *Wallets are exposed to various security threats.*

Onther Inc.

Problem 2: Usability Concerns



Onther Inc.

Solution : ERC 4337 + Webauthn API(FIDO2)

Challenges:

1. Popularized wallets have security vulnerabilities.
2. To use blockchain wallets, a high learning curve exists – a barrier to widespread blockchain adoption.

Solutions:

1. The smart contract(ERC 4337) wallet effectively tackles Usability Concerns.
2. The WebAuthn API(FIDO2) provides solutions to Security Issues.

Onther Inc.

ERC-4337

ERC-4337(Account Abstraction, AA)

ex)
I have in my possession an NFT called 'Covid Alien,' valued at 13 billion. It is secured by my private key, allowing for its transfer at any time.

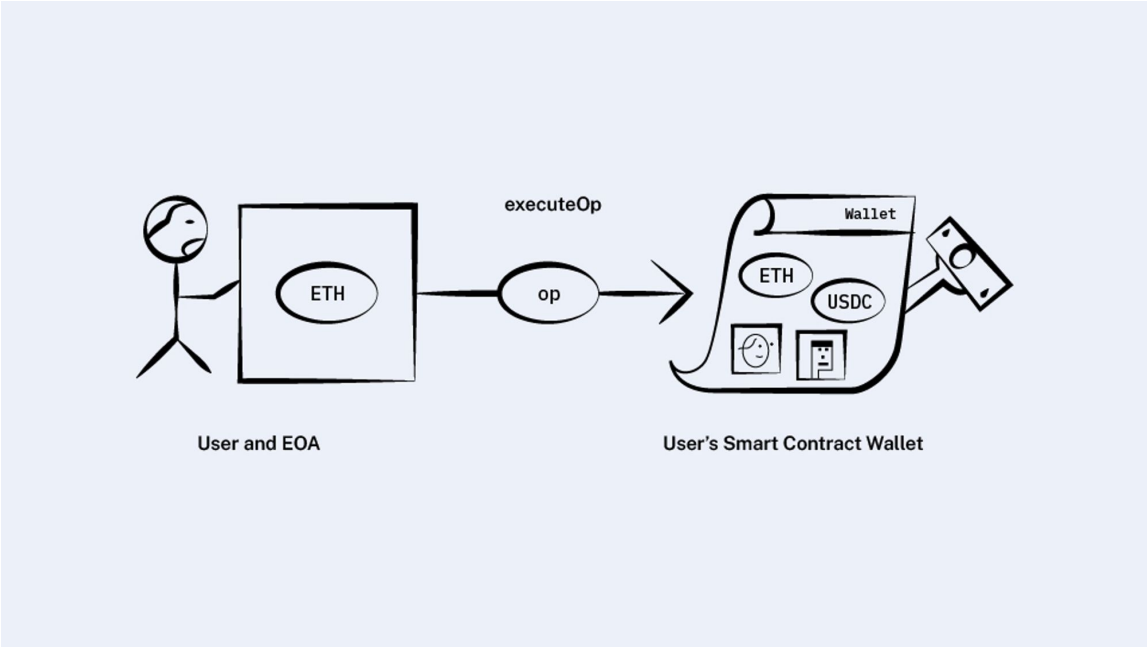
However, this also means that if someone were to access this private key, they would have the ability to transfer this valuable NFT.

Covid Alien #7523(CryptoPunk)

- What if we could add desired functionalities to an EOA (Externally Owned Account)?
- In other words, if a smart contract wallet were to exist?

Onther Inc.

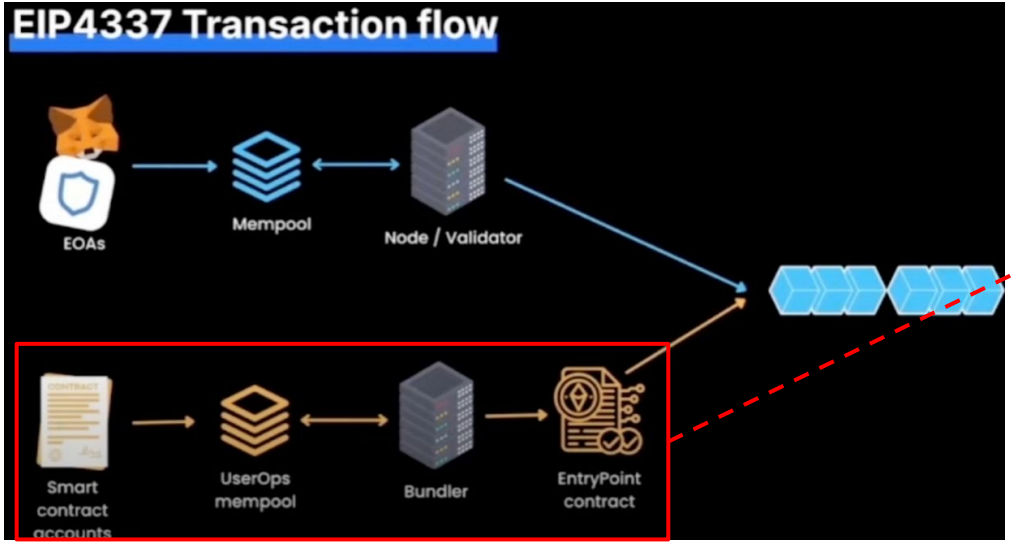
ERC-4337

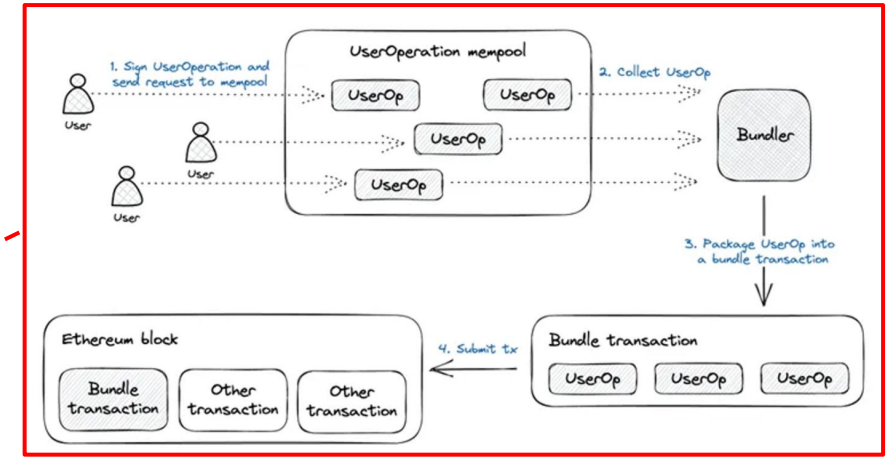


Ultimately, both an 'EOA' and a 'Smart Contract' Wallet are necessary.

Smart Contract Project

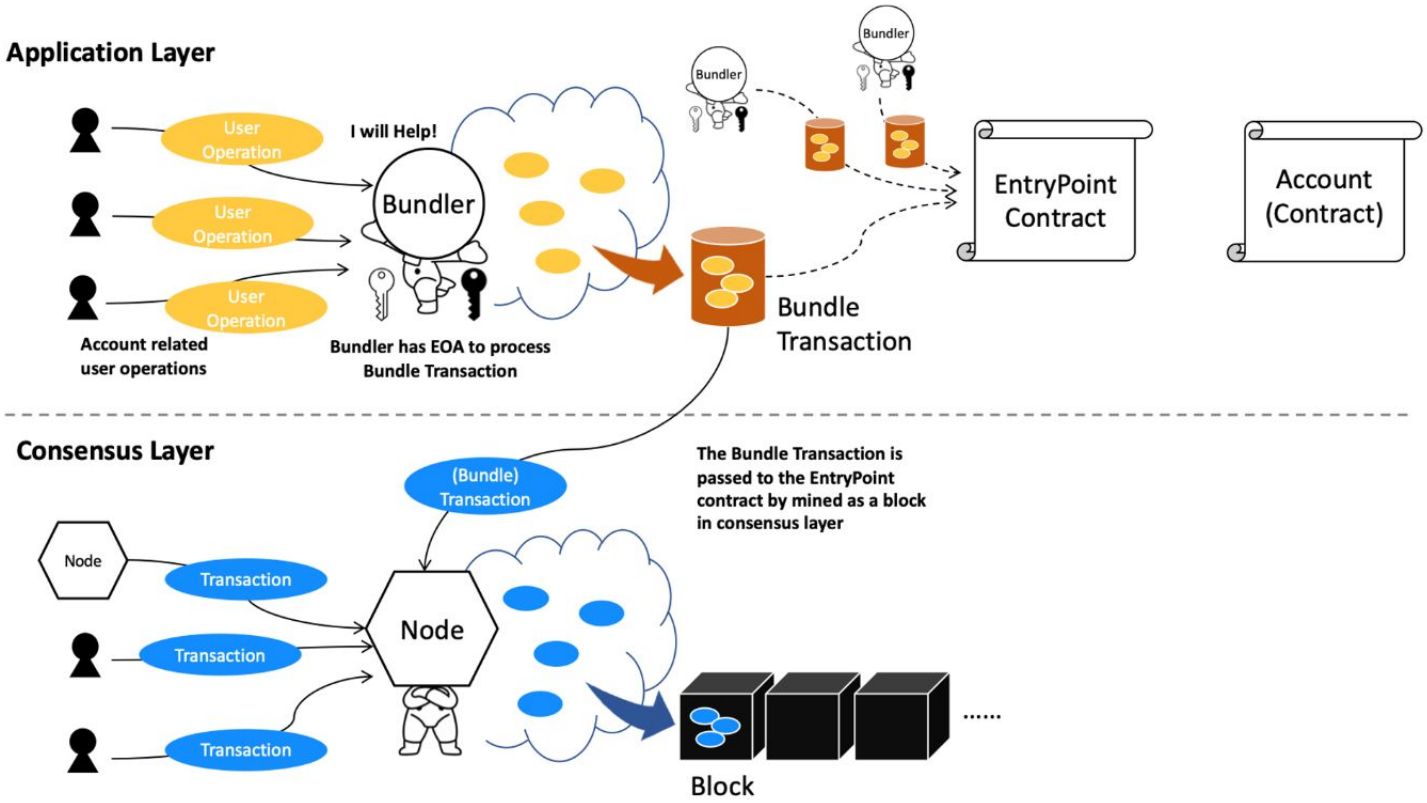
ERC-4337





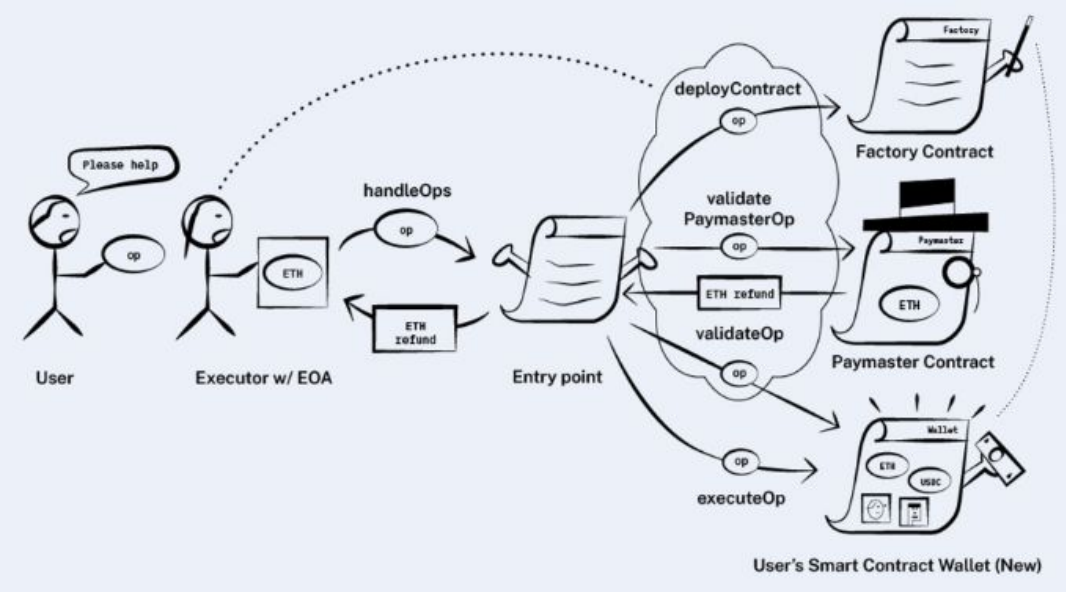
Onther Inc.

ERC-4337



Onther Inc.

ERC-4337



- The transaction I sign can be executed by someone else, thanks to the presence of bundlers.
- By turning my wallet into a smart contract, (account abstraction) it's possible to create a EOA even if one doesn't exist.
- If there's no gas fee available, the gas fee can be paid on my behalf (gas fee abstraction).
- Since the wallet is made as a smart contract, functionalities can be added.
- For example, the signing algorithm can be changed to any algorithm of my choice (signature abstraction).

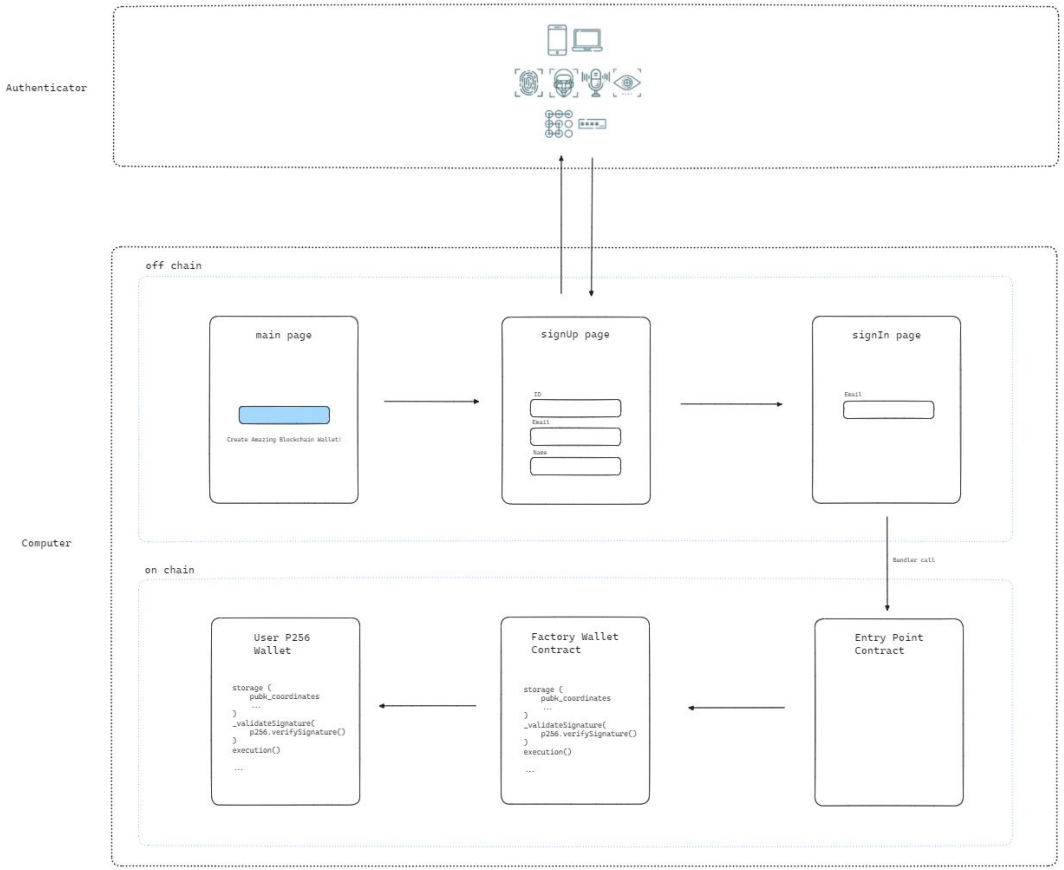
Onther Inc.

Partial Summary

1. As a smart contract wallet, it allows for the flexible implementation of features (account abstraction).
2. The signing function can utilize algorithms of choice (signature abstraction).
3. The presence of bundlers enables transaction execution without an EOA.
4. The existence of paymasters allows for the abstraction of gas fees (gas fee abstraction).

Onther Inc.

Implementation



Onther Inc.

Implementation

- **What in the ETH App ecosystem excites me 2022.12** (link)
  - In December 2022, it was highlighted that current wallets in the Ethereum ecosystem force users to make a tough choice between convenience and security, often leading to a compromised experience.
  - The emergence of ERC-4337 and account abstraction wallets presents a promising alternative, offering an opportunity to overcome this dilemma.

- **Some personal user experiences 2023.2** (link)
  - In February 2023, Vitalik Buterin shared his personal experiences with blockchain services. He discussed his unsuccessful attempt with a social recovery wallet based on Shamir's Secret Sharing.
  - As a solution, he pointed to the potential of using account abstraction wallets, emphasizing the necessity of ERC-4337 for enhancing user experience and security.

Onther Inc.

Implementation

Demo

Onther Inc.

Thank you