ACM CCS 2024
Salt Lake City, USA

Stealing Trust: Unraveling Blind Message Attacks in Web3 Authentication

Kailun Yan [1,2] Xiaokuan Zhang [2] Wenrui Diao [1]

1. Shandong University; 2. George Mason University

Contact:
Kailun Yan
kailun@mail.sdu.edu.cn

Image generated by ChatGPT.

ACM CCS 2024
Salt Lake City, USA

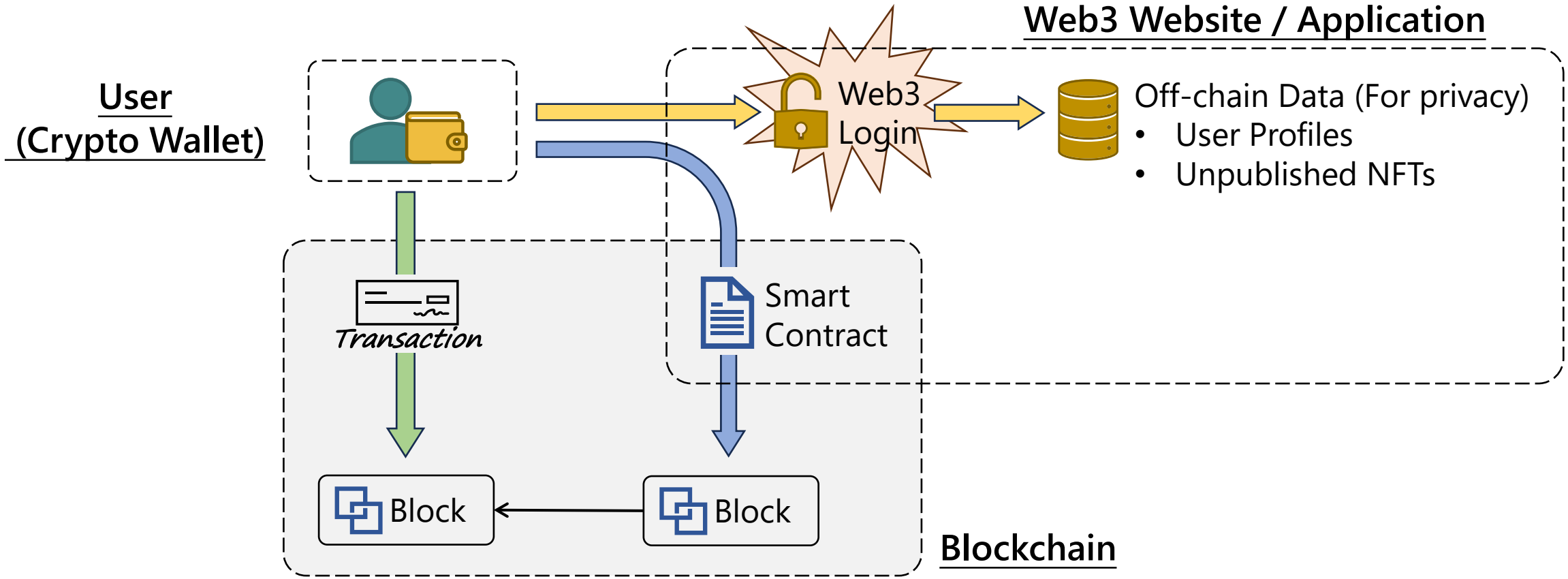
Background: Web3 Ecosystem

- ✓ **User-owned Data**
  Data controlled by users (via blockchain)
- ✓ **Decentralized Identity**
  Managed by users themselves (public-private key pairs)
- ✓ **Secured by cryptography**
  Enhanced security via cryptography and decentralization
- ✓ **Self-governance**
  Governed by users (e.g., DAOs through token voting)

Web3 Applications

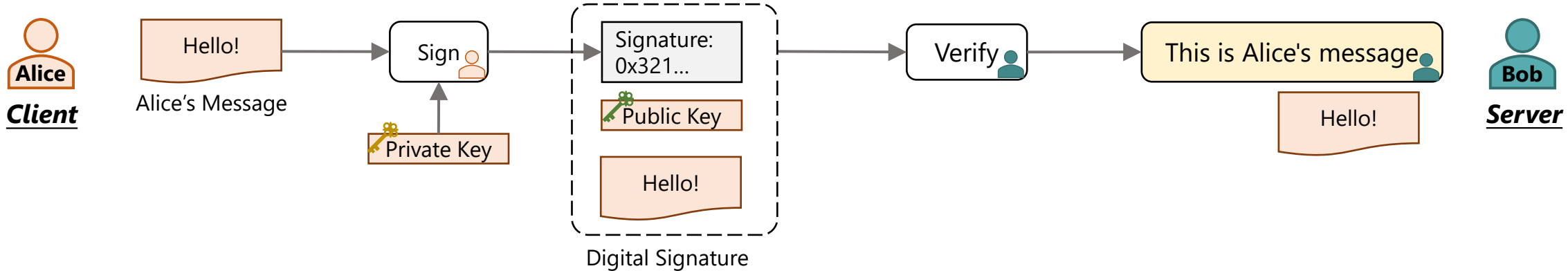
- DeFi (Decentralized Finance) *over 100 billion USD!*
- NFTs (Non-Fungible Tokens)

Background: Web3 Ecosystem



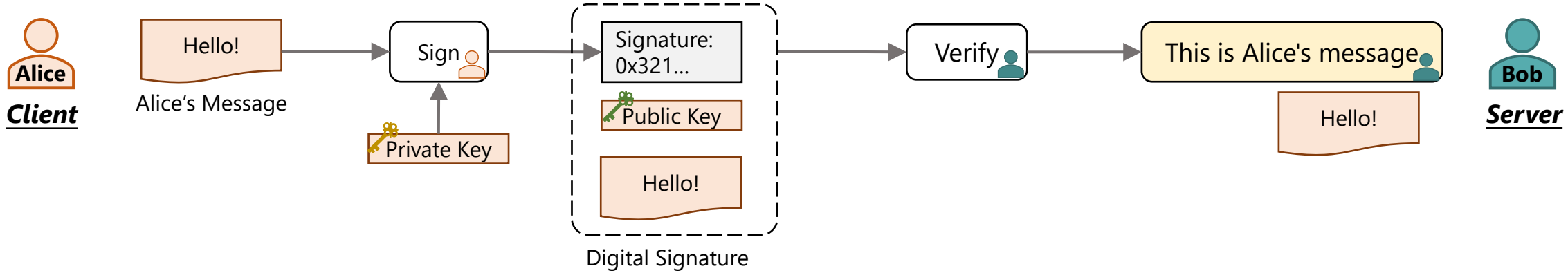
Background: Web3 Login

- Digital Signature: Validity of Message

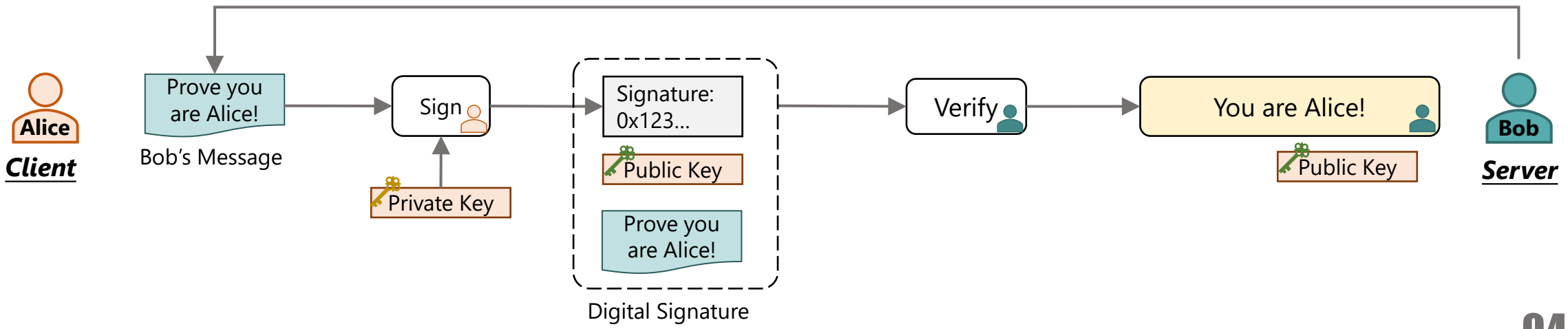


Background: Web3 Login

➢ Digital Signature: Validity of Message



➢ Web3 Login: Validity of Address (Public key)

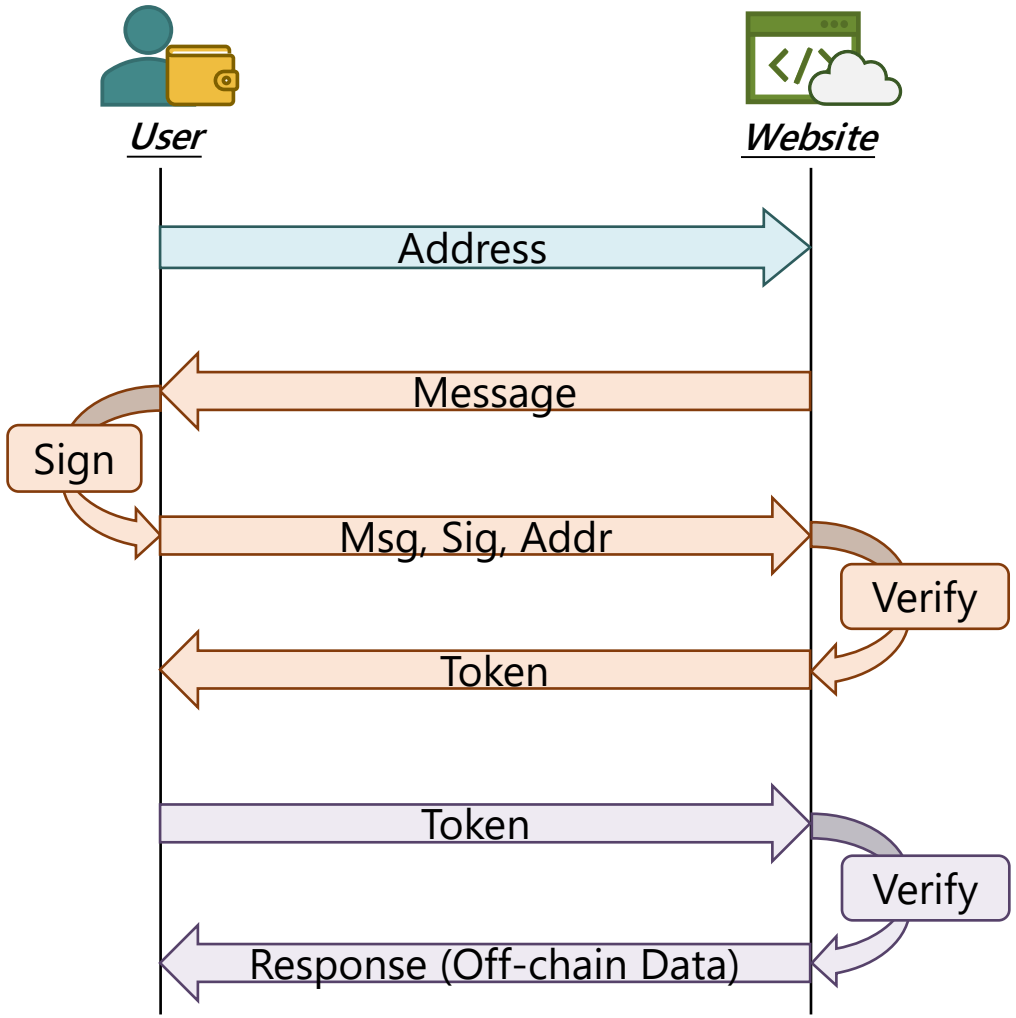


Web3 Login Workflow

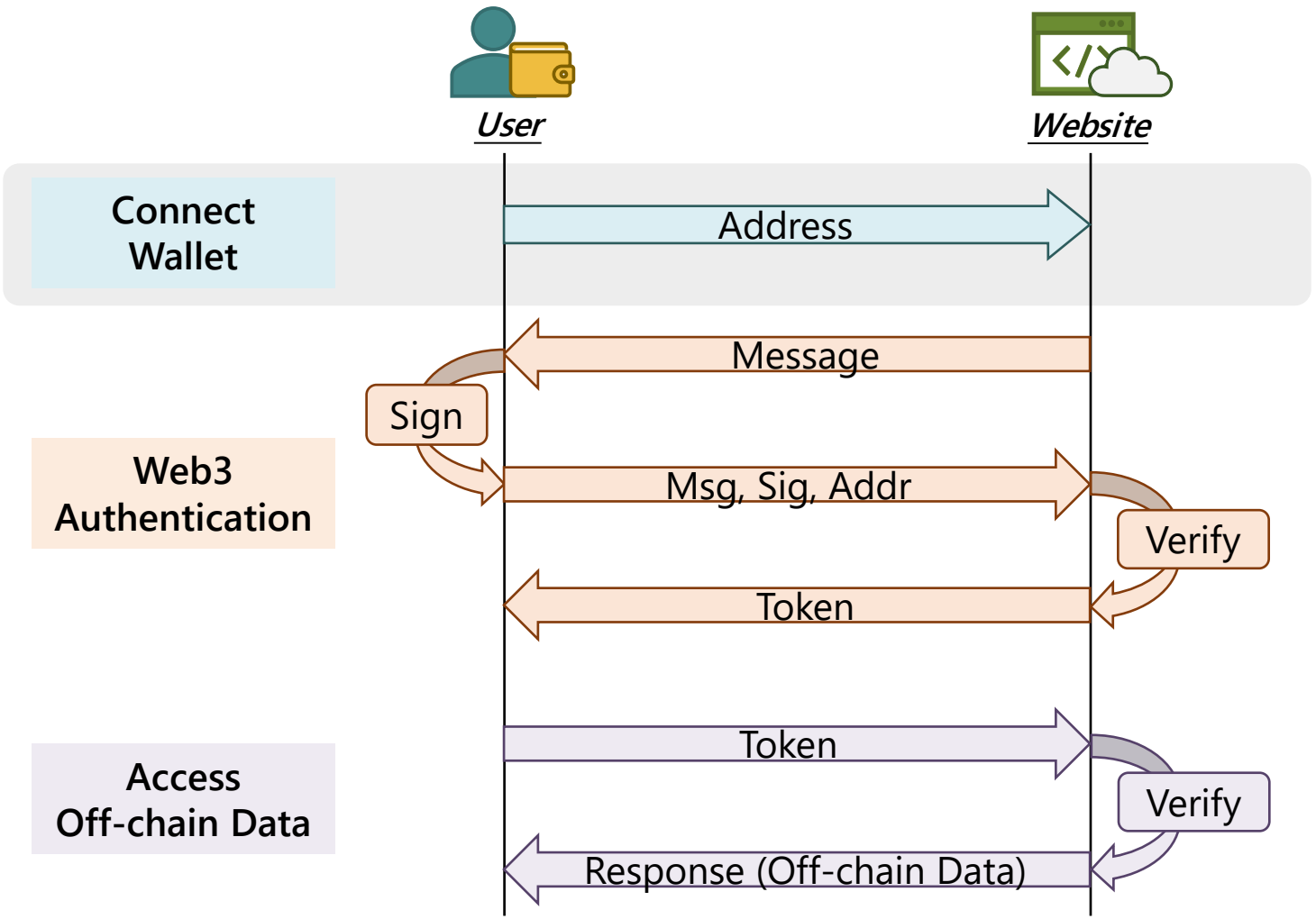
Connect Wallet

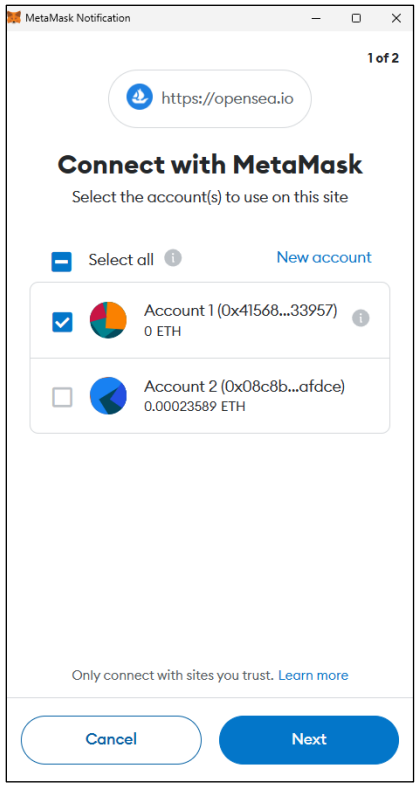
Web3 Authentication

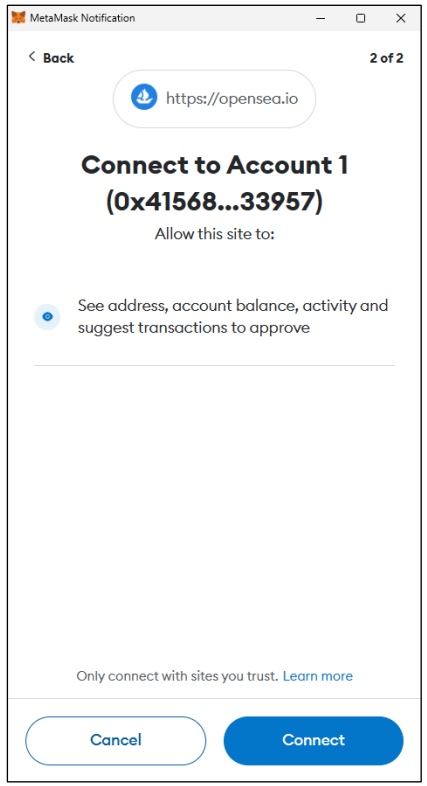
Access Off-chain Data



Web3 Login Workflow

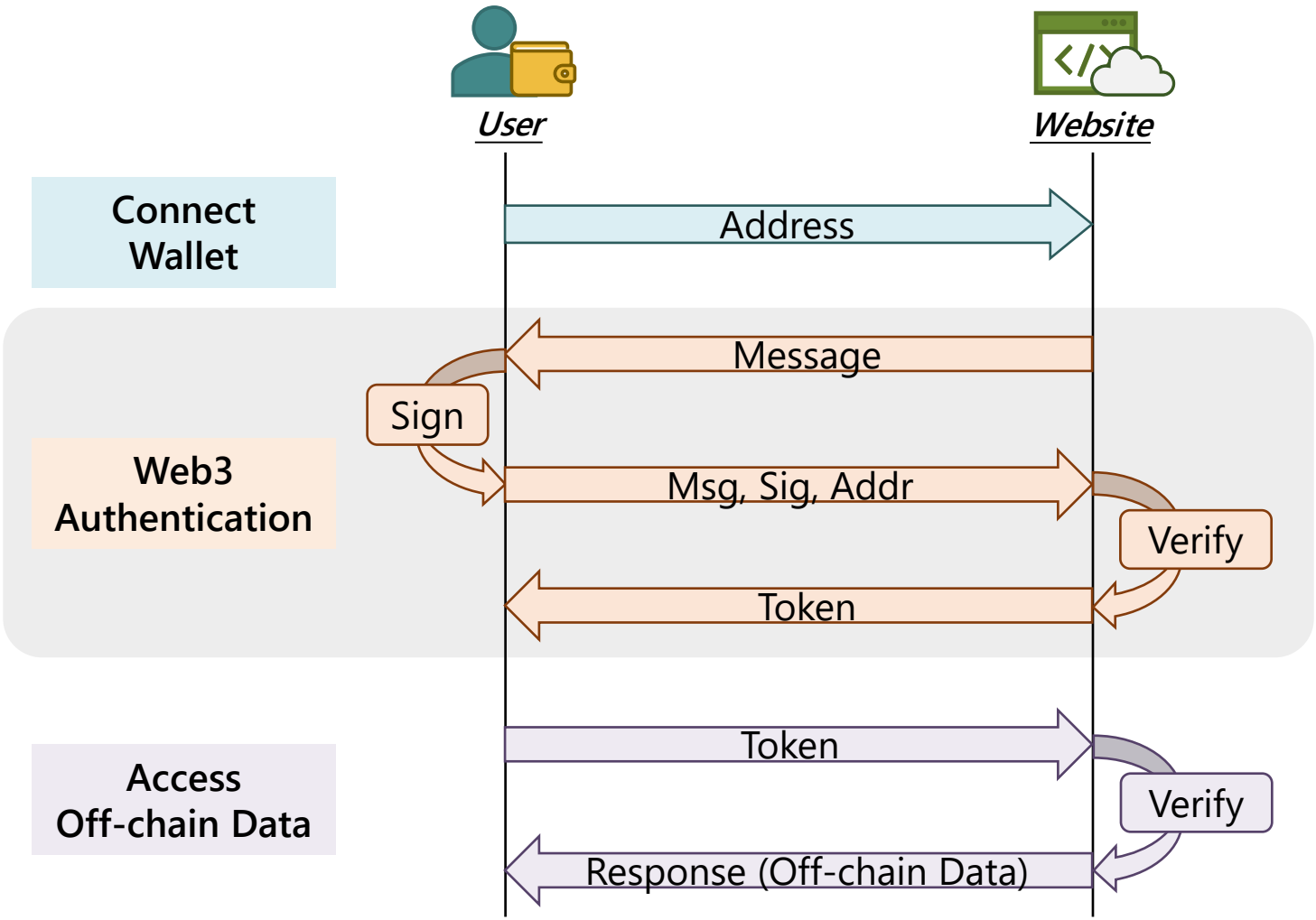


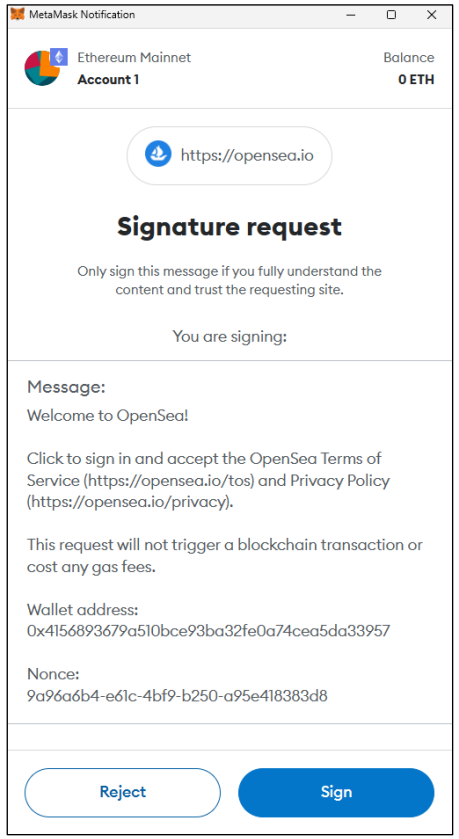




Connect with Metamask

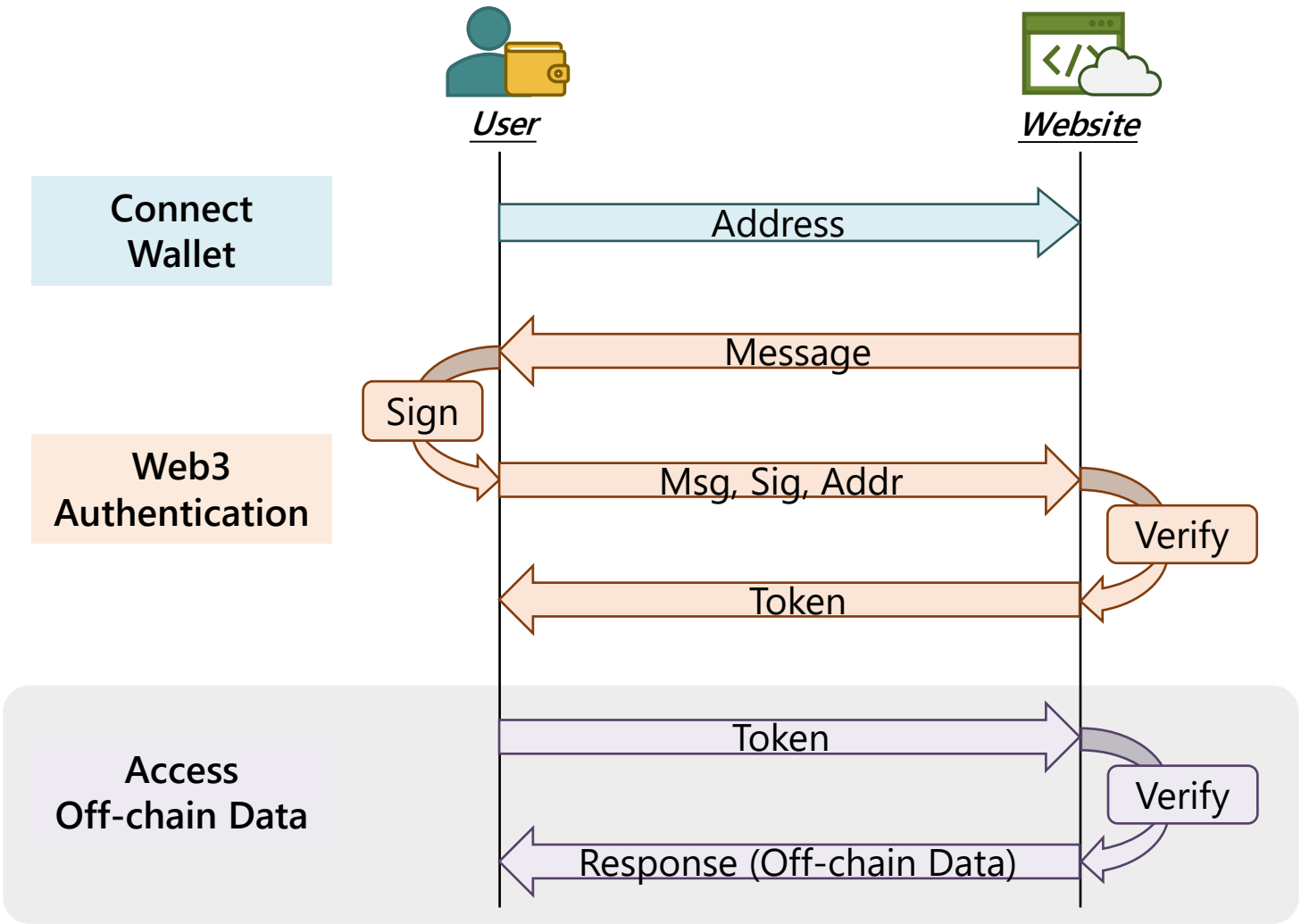
Web3 Login Workflow

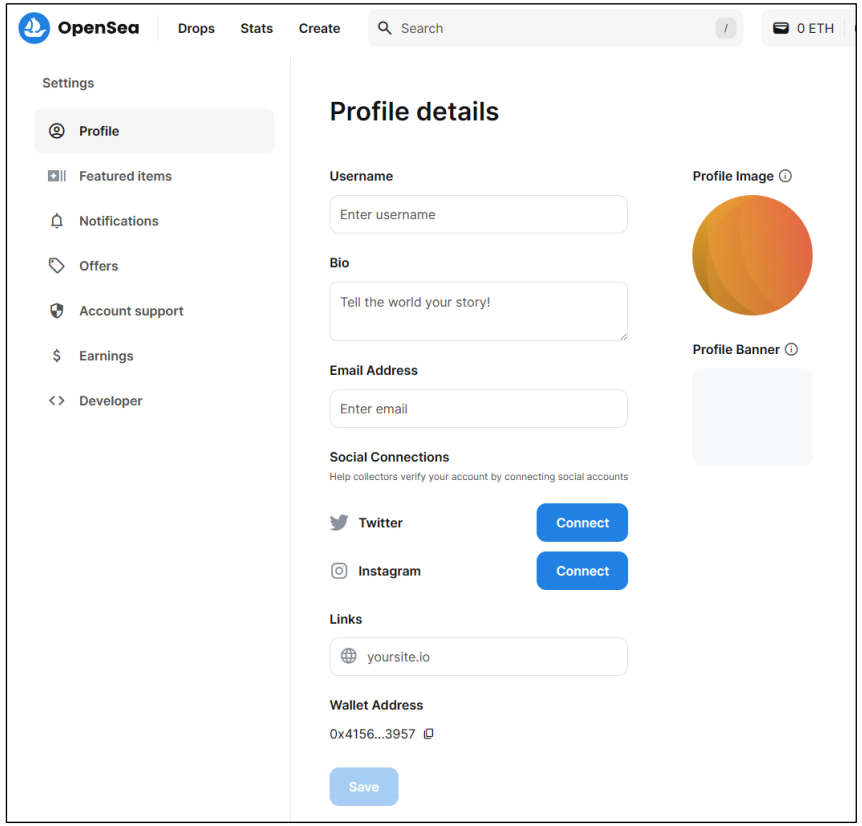




Signature Page

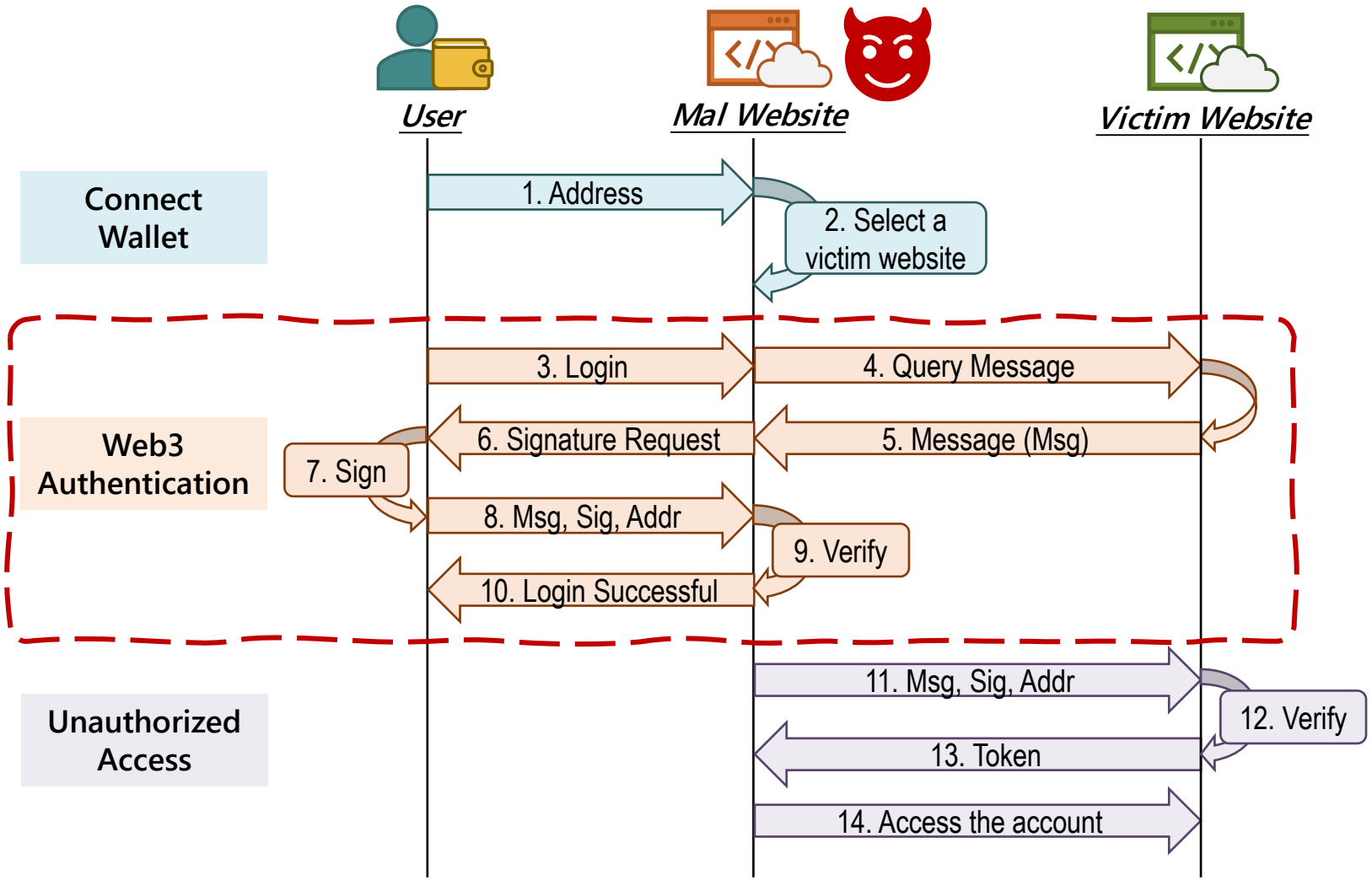
Web3 Login Workflow





Profile Page (Opensea.io)

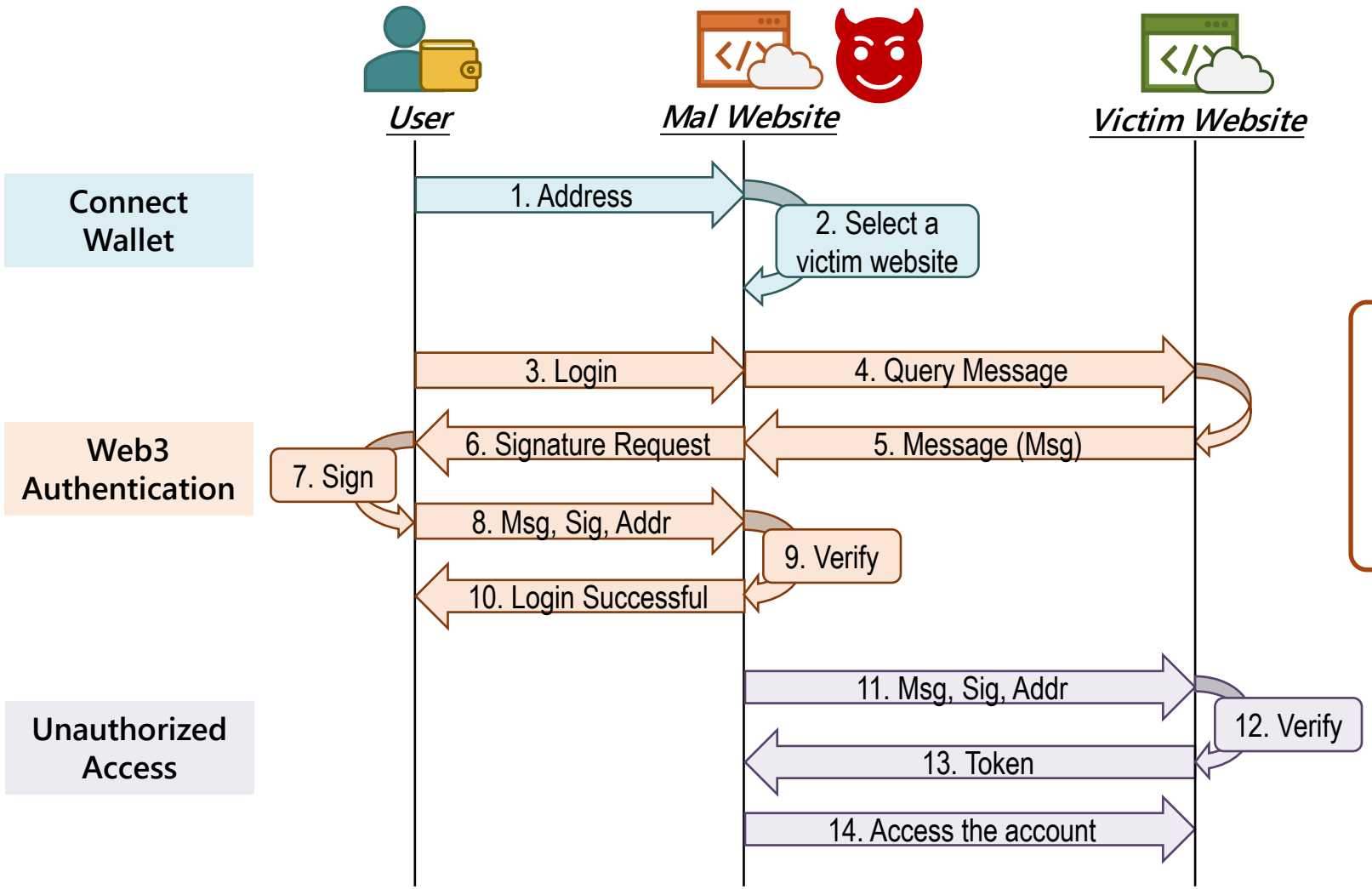
Threat Model



Malicious Applications/Websites:
Exploit vulnerabilities in Web3 login to steal a user's identity.

Attacker Goal:
Gain unauthorized access to the victim website.

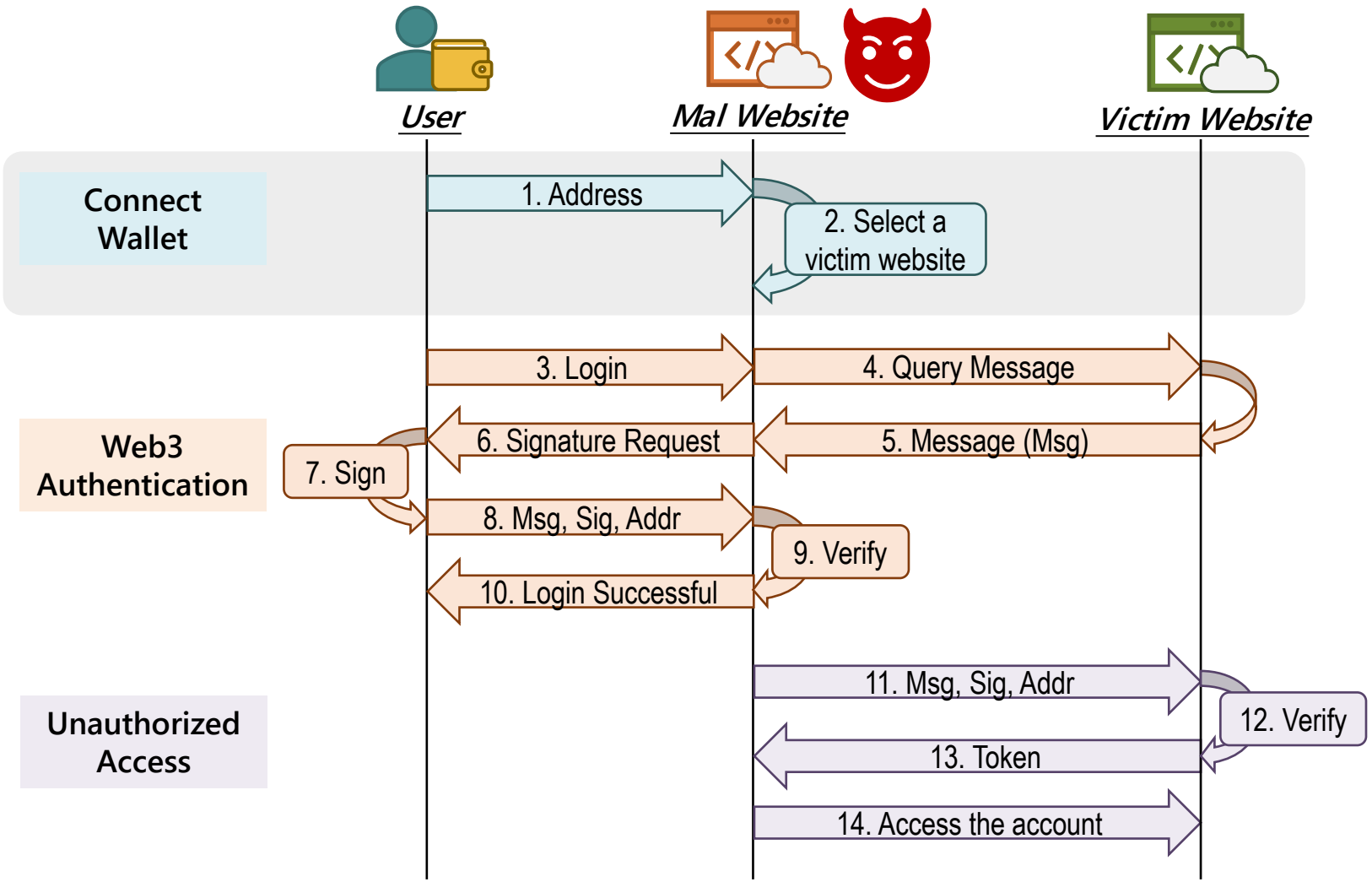
Blind Message Attack (BMA)



Blind Message Attack

A malicious website tricks a user into signing a message from another (victim) website, thereby stealing the user's identity.

Blind Message Attack (BMA)

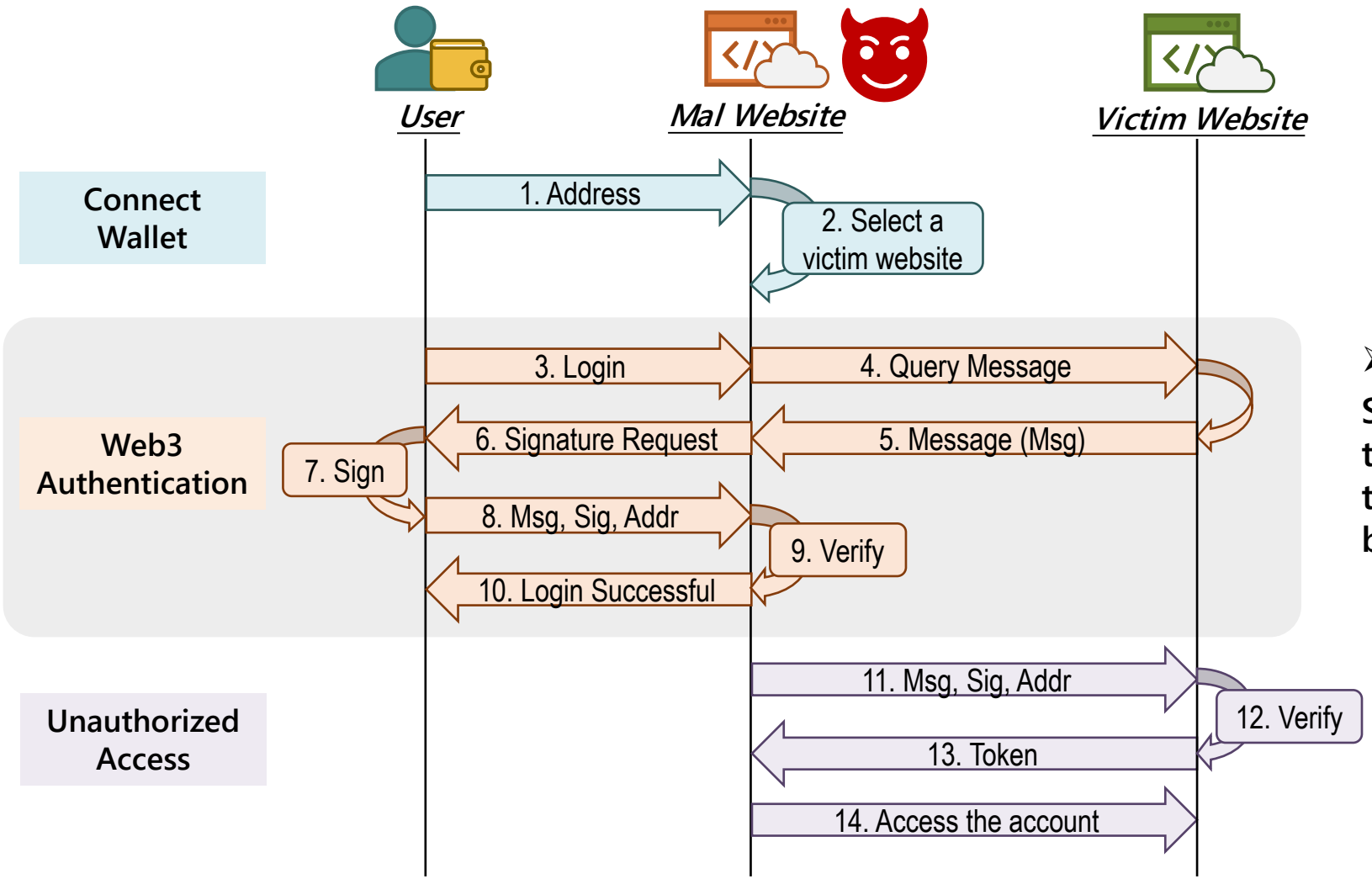


- Select a victim website (Connect Wallet)

Step 1: User connects wallet to mal website

Step 2: Mal website selects a victim website by the address and on-chain data

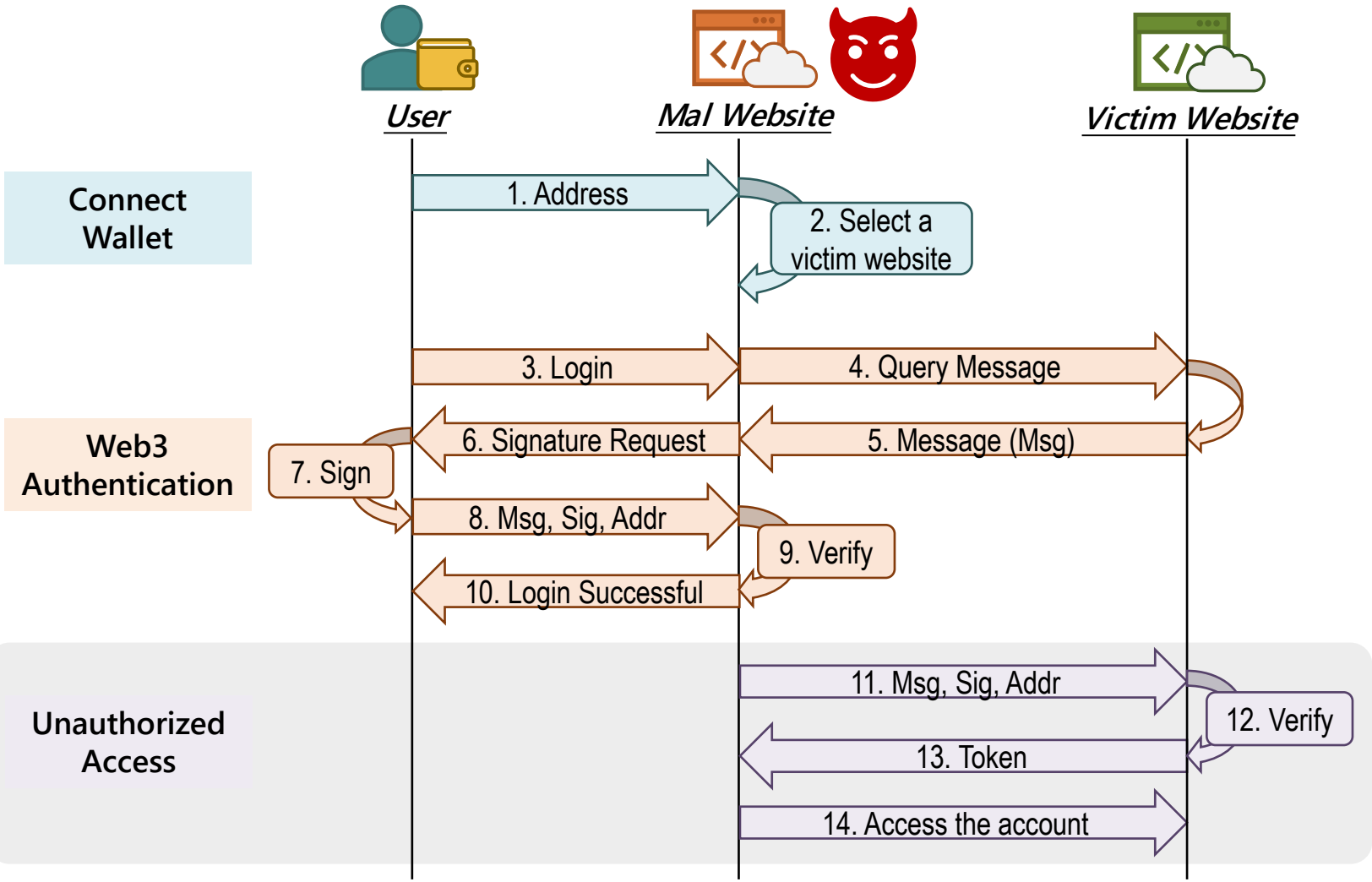
Blind Message Attack (BMA)



- Get the user's signature

Step 3-10: Mal website gets a message from the victim website. The user is unaware that the message is from the victim website and blindly signs it.

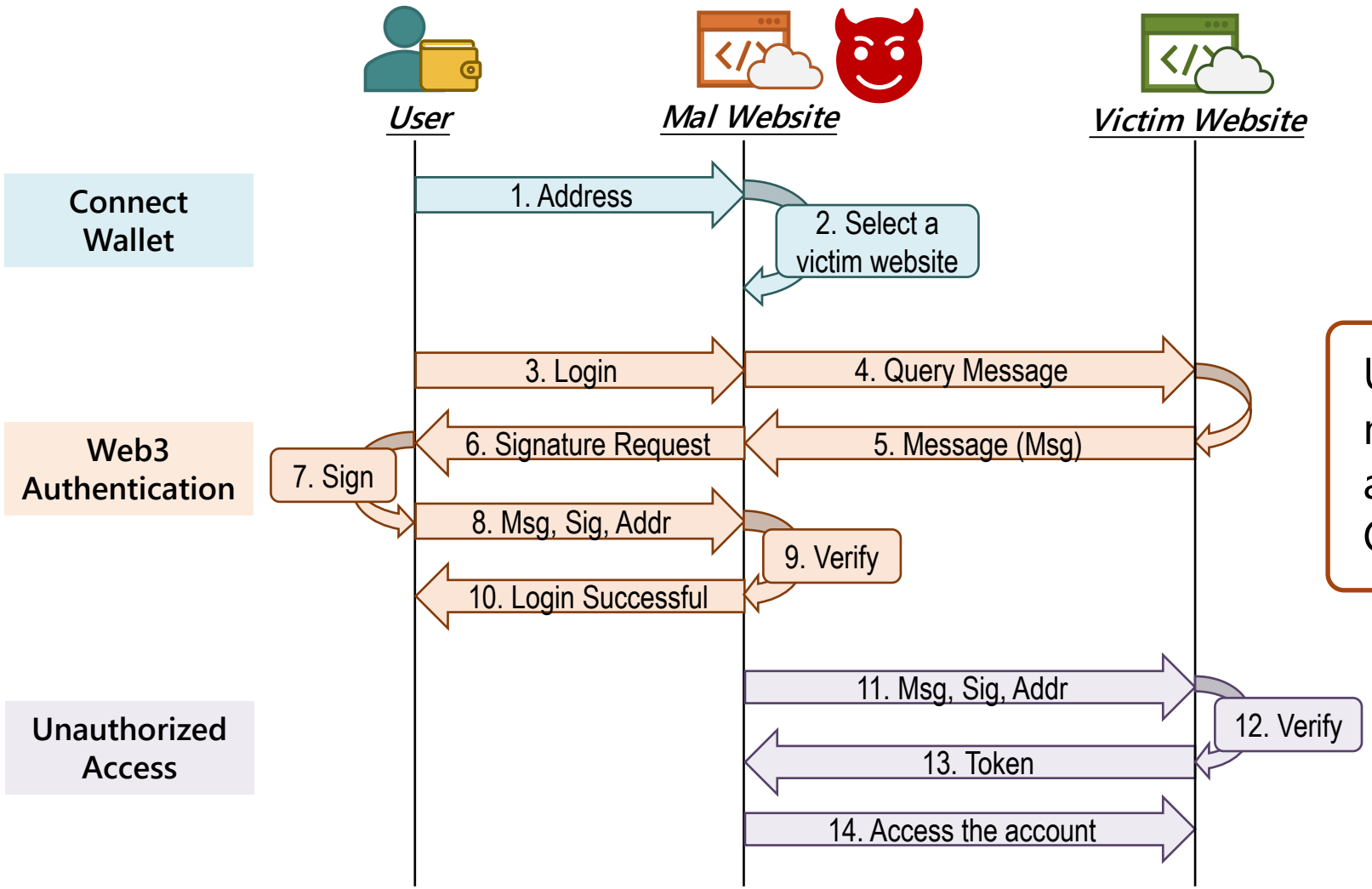
Blind Message Attack (BMA)



- **Unauthorized access**

Step 11-14: Mal website uses the user's signature to access the user's account

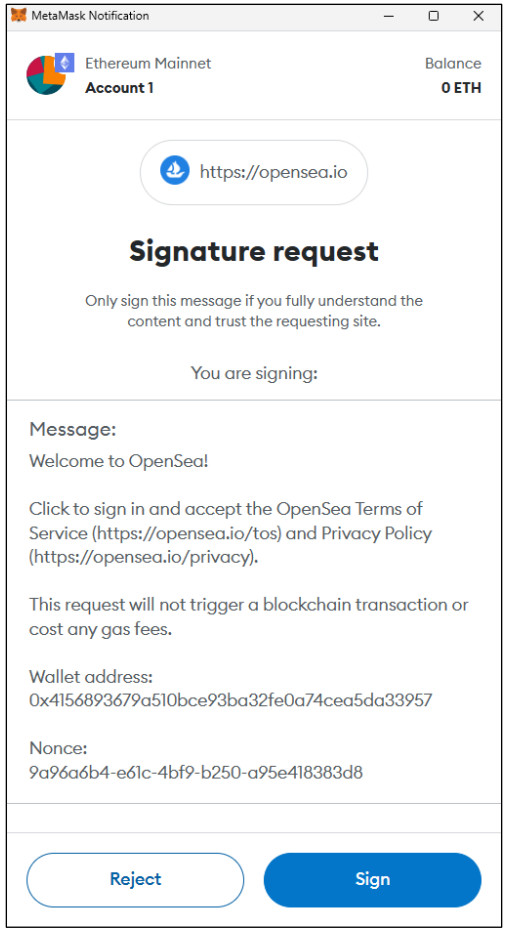
Blind Message Attack (BMA)



Root Cause

Users DO NOT check the source of messages,
and the source of some messages CANNOT be identified by users.

Web3 Login: Message Design

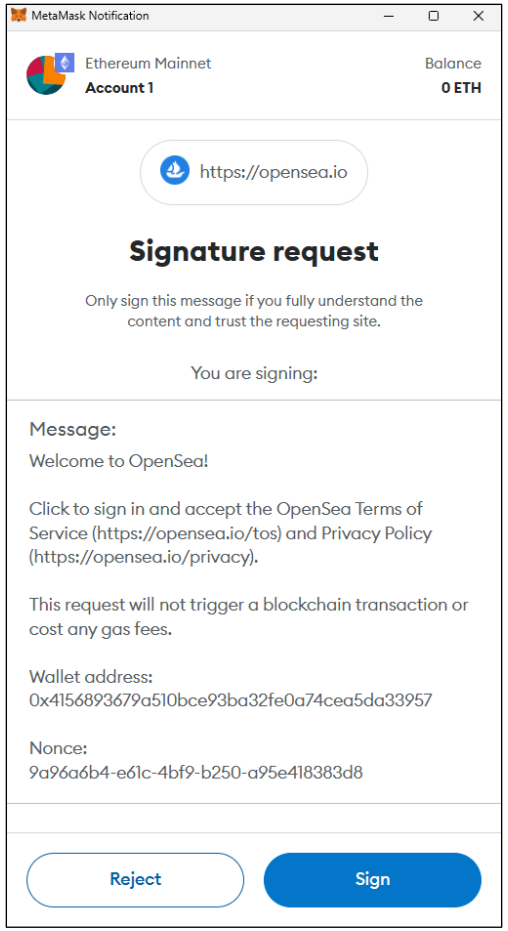


opensea.io

Good Message from opensea.io

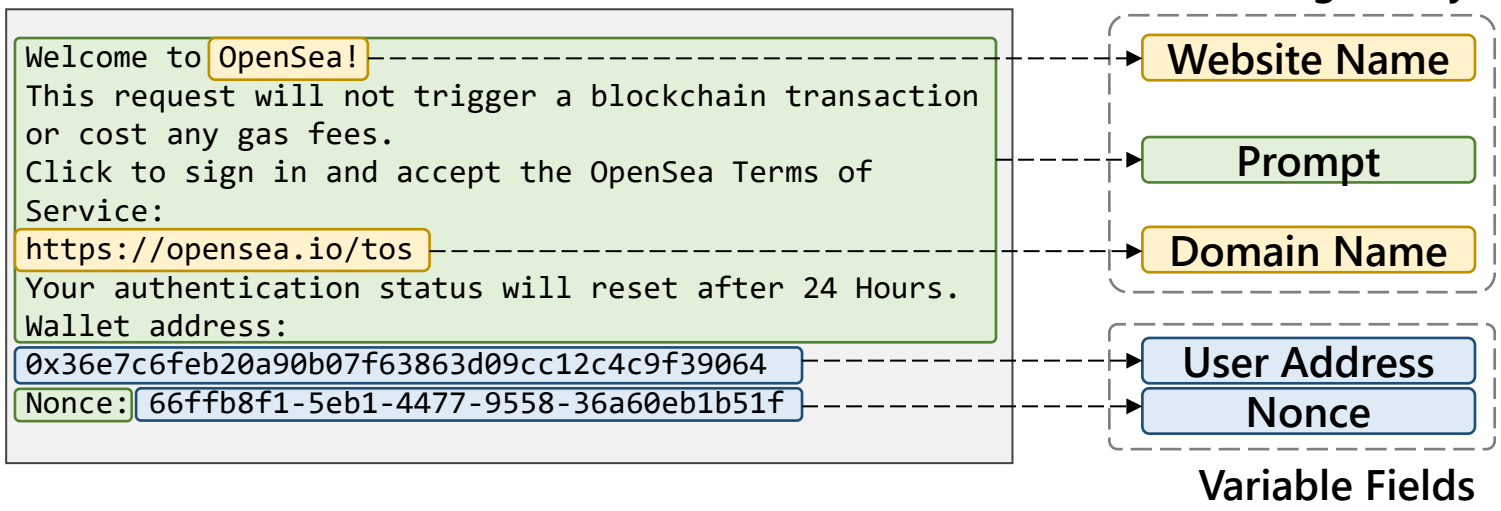
```
Welcome to OpenSea!
This request will not trigger a blockchain transaction
or cost any gas fees.
Click to sign in and accept the OpenSea Terms of
Service:
https://opensea.io/tos
Your authentication status will reset after 24 Hours.
Wallet address:
0x36e7c6feb20a90b07f63863d09cc12c4c9f39064
Nonce: 66ffb8f1-5eb1-4477-9558-36a60eb1b51f
```

Web3 Login: Message Design

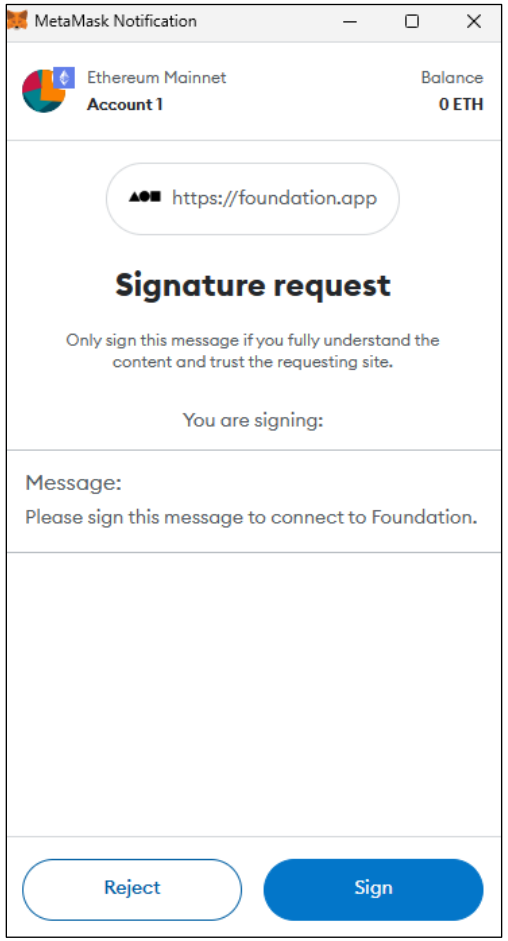


opensea.io

Good Message from opensea.io



Web3 Login: Message Design



foundation.app

Good Message from opensea.io

```
Welcome to OpenSea!
This request will not trigger a blockchain transaction
or cost any gas fees.
Click to sign in and accept the OpenSea Terms of
Service:
https://opensea.io/tos
Your authentication status will reset after 24 Hours.
Wallet address:
0x36e7c6feb20a90b07f63863d09cc12c4c9f39064
Nonce: 66ffb8f1-5eb1-4477-9558-36a60eb1b51f
```

Static Fields (Message Body)

- Website Name
- Prompt
- Domain Name

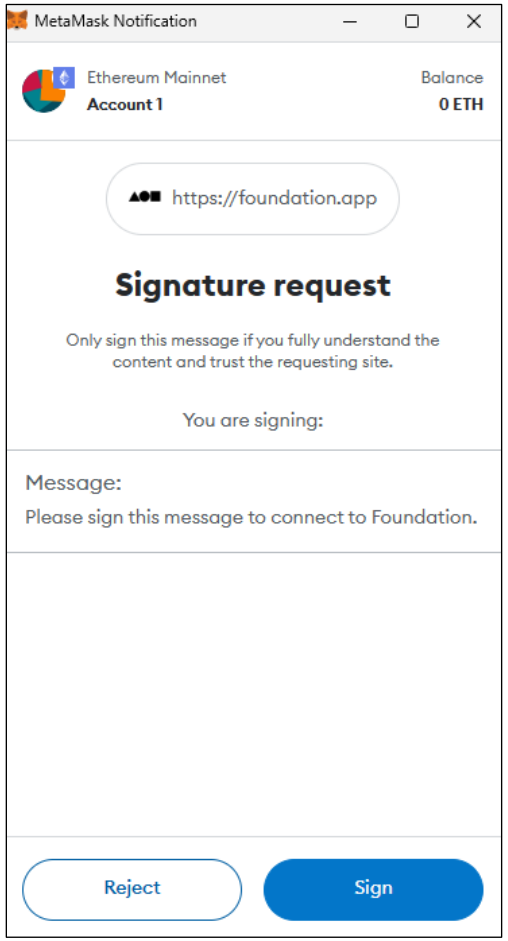
Variable Fields

- User Address
- Nonce

Bad Message from foundation.app

```
Please sign this message to connect to Foundation.
```

Web3 Login: Message Design



foundation.app

Good Message from opensea.io

```
Welcome to OpenSea!
This request will not trigger a blockchain transaction
or cost any gas fees.
Click to sign in and accept the OpenSea Terms of
Service:
https://opensea.io/tos
Your authentication status will reset after 24 Hours.
Wallet address:
0x36e7c6feb20a90b07f63863d09cc12c4c9f39064
Nonce: 66ffb8f1-5eb1-4477-9558-36a60eb1b51f
```

Static Fields (Message Body)

- Website Name
- Prompt
- Domain Name

Variable Fields

- User Address
- Nonce

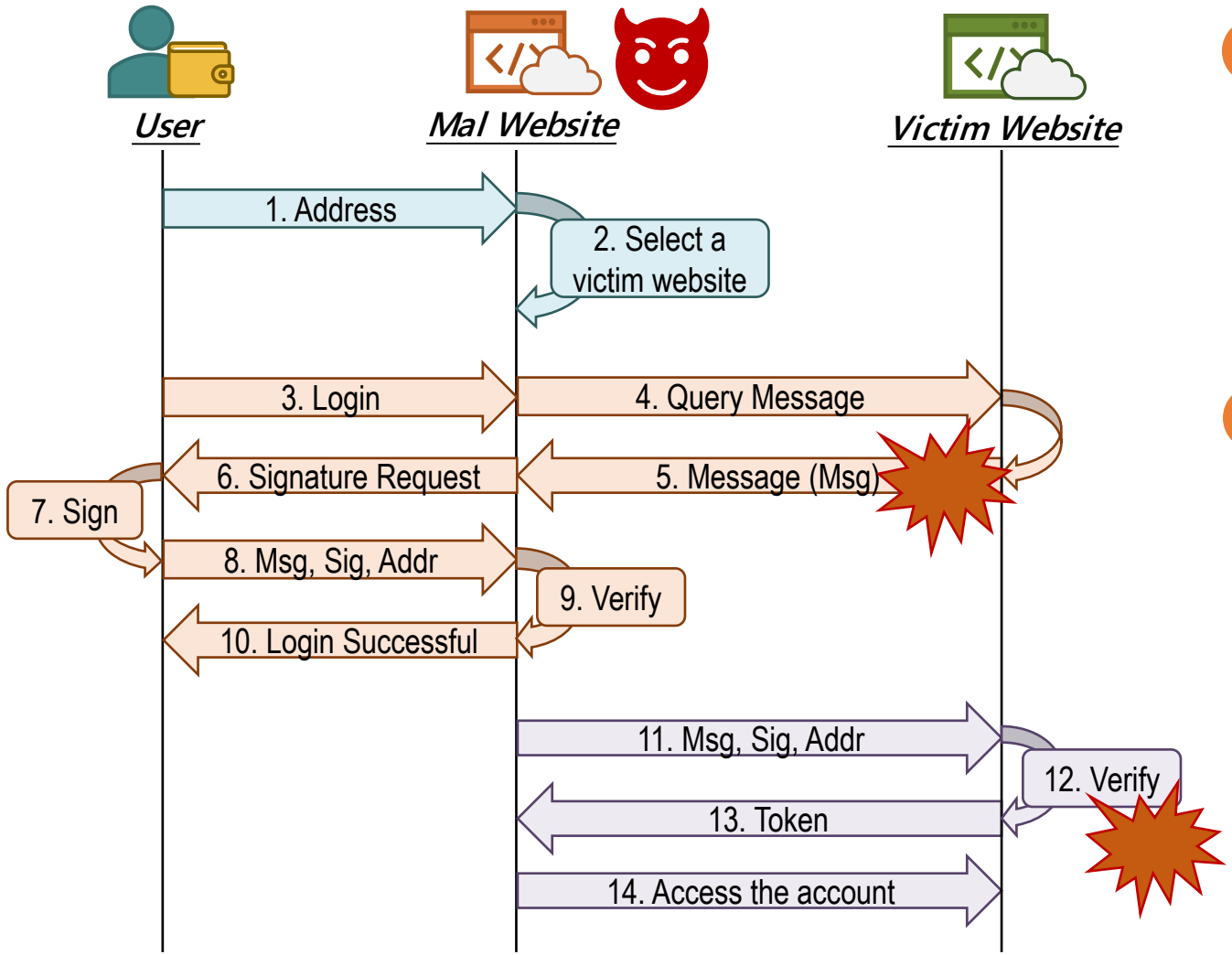
Bad Message from foundation.app

```
Please sign this message to connect to Foundation.
```

Mal Website, such as foundation.com

```
Please sign this message to connect to Foundation.
```

Web3 Login: Vulnerability



Message Design

- × Lack of Domain Name
- × Lack of Website Name
- × Lack of Nonce

Server Verification

- × Unchecked Message
- × Unchecked Message Body
- × Improper Check Message body
- × Unchecked Nonce
- × Unchecked Signature
- × Unchecked Address

Risk Levels

Critical Risk

No interaction required

- × Unchecked Message
- × Unchecked Signature
- × Unchecked Address

High Risk

Users are unable to detect BMA

- × Lack of Domain Name
- × Unchecked Message Body

Medium Risk

Experienced users might detect BMA

- × Improper Check Message body

Low Risk

Careless users might be vulnerable to BMA

Risk Levels

Critical Risk

No interaction required

- × Unchecked Message
- × Unchecked Signature
- × Unchecked Address

High Risk

Users are unable to detect BMA

- × Lack of Domain Name
- × Unchecked Message Body

Medium Risk

Experienced users might detect BMA

- × Improper Check Message body

Low Risk

Careless users might be vulnerable to BMA

Critical-Risk Example

LearnBlockchain.cn

```
Learnblockchain.
```

- × Lack of Domain Name
- × Lack of Nonce
- × Unchecked Message

Attackers can use any signature of the user to pass the server verification.

Blind Multi-Message Attacks

The attacker can use a single signature to access multiple victim websites.

Foundation.com (Malicious Website)

```
Welcome!
Please sign this message to connect to Foundation.com.

Web3 Token Version: 2
Nonce: 60537526
Issued At: 2024-10-15T14:18:13.016Z
Expiration Time: 2024-10-16T14:18:13.000Z

Timestamp: 1788528015
```

Blind Multi-Message Attacks

The attacker can use a single signature to access multiple victim websites.

Foundation.com (Malicious Website)

```
Welcome!
Please sign this message to connect to Foundation.com.

Web3 Token Version: 2
Nonce: 60537526
Issued At: 2024-10-15T14:18:13.016Z
Expiration Time: 2024-10-16T14:18:13.000Z

Timestamp: 1788528015
```

Foundation.app

```
Please sign this message to connect to Foundation.
```

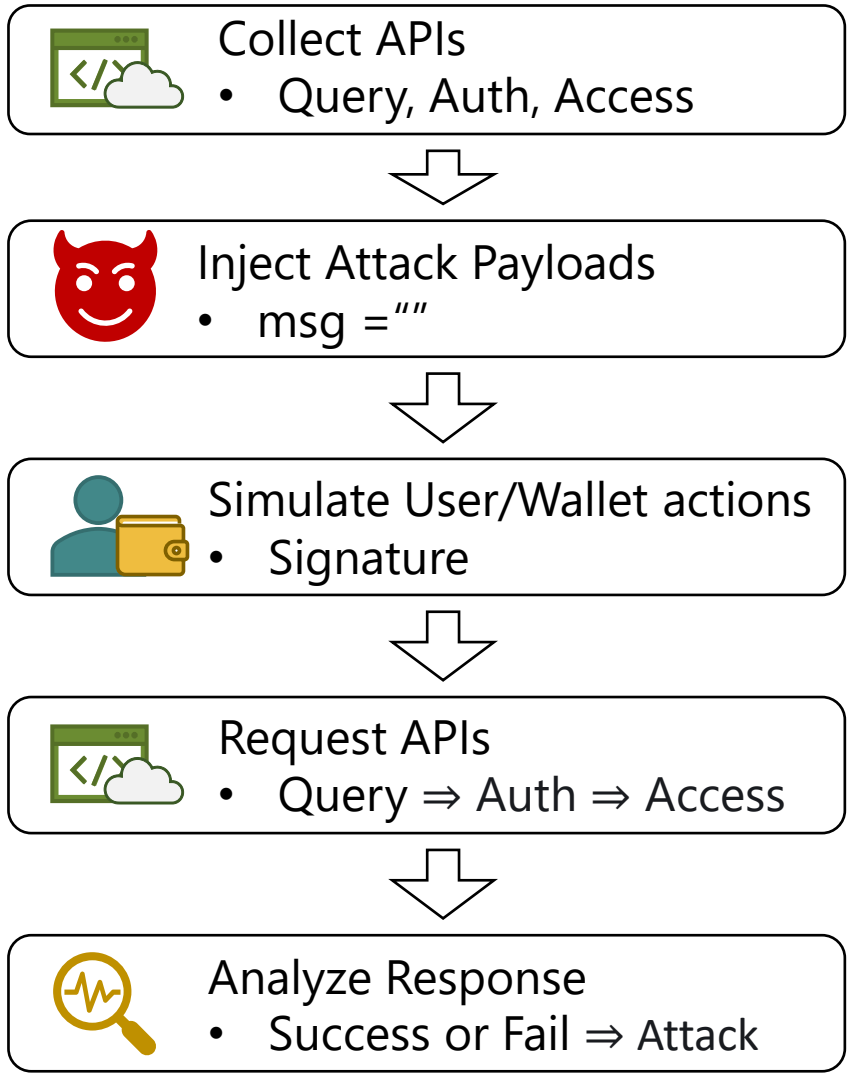
Planetix.com × Unchecked Message Body

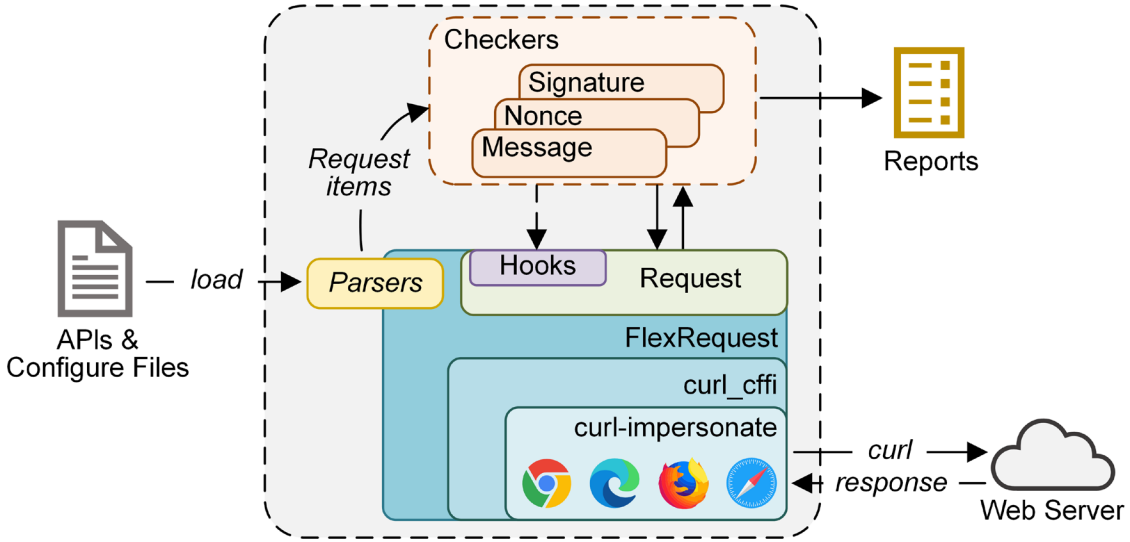
```
URI: https://planetix.com/connect
Web3 Token Version: 2
Nonce: 60537526
Issued At: 2024-10-15T14:18:13.016Z
Expiration Time: 2024-10-16T14:18:13.000Z
```

QuestN.com × Unchecked Message Body

```
Welcome to QuestN.
Please sign this message to login QuestN.
Timestamp: 1788528015
```

Detection: Web3AuthChecker





Dataset

DappRadar

- 29 Cases
  - 25 User login
  - 4 Update Profile

Results

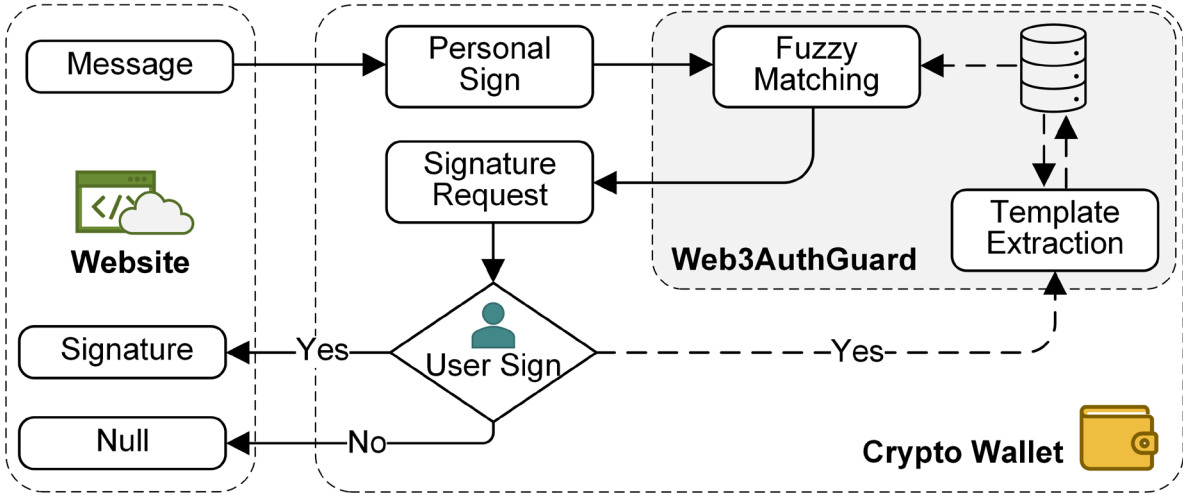
- Critical: 2
- High: 13
- Medium: 7
- Low: 7

22/29

#	Website	Cat.	30d Vol.	Design			Implementation (Verification)					Security Risk		
				Domain	Name	Nonce	Message	Body	Nonce	Signature	Address	BMA	RA	BMMA
1	Blur	Mkt.	$522.59M	✘	✓	✓	✓	✓	✓	✓	✓	M	○	○
2	OpenSea	Mkt.	$104.35M	✓	✓	✓	✓	✓	✓	✓	✓	L	○	○
3	LooksRare	Mkt.	$67.29M	✓	✓	✓	✓	✓	✓	✓	✓	L	○	○
4	Foundation	Mkt.	$1.77M	✘	✓	✘	✓	✘(II)	N/A	✓	✓	M	●	●
5	Element	Mkt.	$1.29M	✓	✓	✓	✓	✘(II)	✓	✓	✓	M	○	●
6	Rarible	Mkt.	$262.63k	✓	✓	✓	✓	✓	✓	✓	✓	L	○	○
7	Joepegs	Mkt.	$194.92k	✘	✓	✓	✓	✓	✓	✓	✓	M	○	○
8	Quix	Mkt.	$160.44k	✘	✘	✓	✓	✘(I)	✘(II)	✓	✓	H	●	●
9	Minted Network	Mkt.	$72.36k	✓	✓	✓	✓	✓	✓	✓	✓	L	○	○
10	Campfire	Mkt.	$40.79k	✓	✓	✓	✓	✓	✓	✓	✓	L	○	○
11	Moonflow NFT	Mkt.	$28.54k	✘	✓	✓	✓	✓	✓	✓	✓	M	○	○
12	Galler	Mkt.	$4.49k	✓	✓	✓	✘	✘(I)	✘(I)	✓	✓	C	●	●
13	PlayDapp	Mkt.	$3.03k	✘	✘	✘	✓	✓	N/A	✓	✓	H	●	○
14	Refinable	Mkt.	$1.81k	✘	✘	✓	✓	✓	✓	✓	✓	H	○	○
15	Apeiron	Mkt.	$331.49	✘	✘	✓	✓	✓	✓	✓	✓	H	○	○
16	Lifty	Mkt.	-	✓	✓	✓	✓	✓	✓	✓	✓	L	○	○
17	LearnBlockchain	Com.	-	✘	✓	✘	✘	✘(I)	N/A	✓	✓	C	●	●
18	DappRadar	Rnk.	-	✘	✘	✓	✓	✓	✓	✓	✓	H	○	○
19	QuestN	Srv.	-	✘	✓	✓	✓	✘(I)	✓	✓	✓	H	○	●
20	Galxe	Soc.	-	✓	✓	✓	✓	✓	✘(I)	✓	✓	L	●	○
21	Planetix	Gme.	-	✓	✓	✓	✓	✘(I)	✘(I)	✓	✓	H	●	●
22	MOBOX	Gme.	-	✘	✘	✓	✓	✓	✓	✓	✓	H	○	○
23	Bomb Crypto 2	Gme.	-	✘	✘	✓	✓	✓	✓	✓	✓	H	○	○
24	Decert	Srv.	-	✘	✓	✓	✓	✓	✓	✓	✓	M	○	○
25	Paragraph	Med.	-	✘	✓	✓	✓	✓	✓	✓	✓	M	○	○
10*	Campfire	Mkt.	-	✘	✘	✘	✓	✓	N/A	✓	✓	H	●	○
17*	Lifty	Mkt.	-	✘	✘	✘	✓	✓	N/A	✓	✓	H	●	○
26*	NFTmall	Mkt.	-	✘	✘	✘	✓	✓	N/A	✓	✓	H	●	○
27*	Babylons	Mkt.	-	✘	✘	✘	✓	✓	N/A	✓	✓	H	●	○

In this table, Cat. = Category, Mkt. = Marketplace, Com. = Community, Rnk. = Ranking, Soc. = Social, Gme. = Game, Med. = Media, Srv. = Service, BMA = Blind Message Attack, RA = Replay Attack, BMMA = Blind Multi-Message Attack.
The website 10*, 17*, 26* and 27* require Web3 authentication when updating profiles.
✓: No vulnerability found; ✘: Vulnerability found; N/A: Not applicable; C: Critical; H: High; M: Medium; L: Low; ●: Risk exists; ○: No risk.

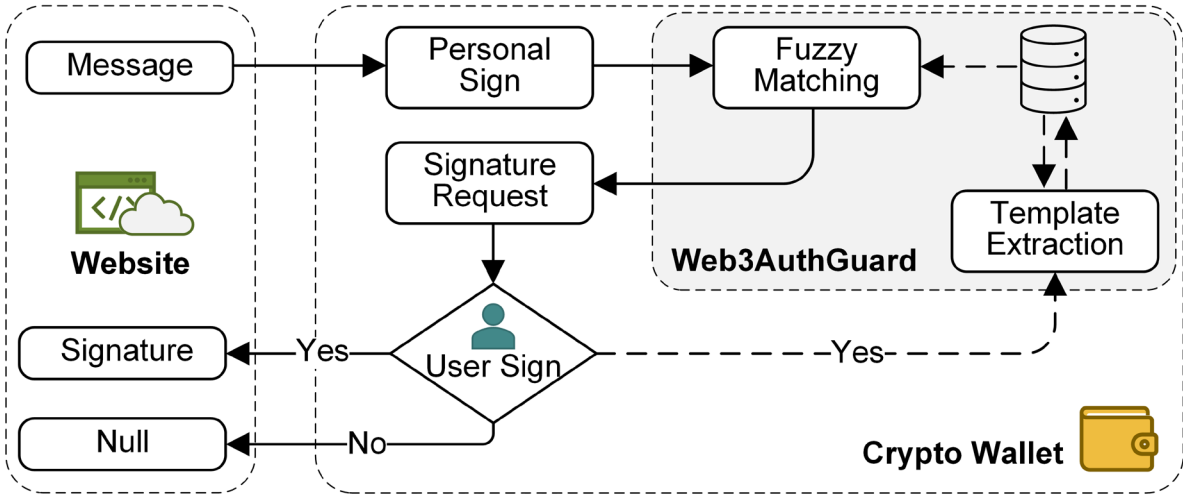
Client-Side Mitigation: Web3AuthGuard



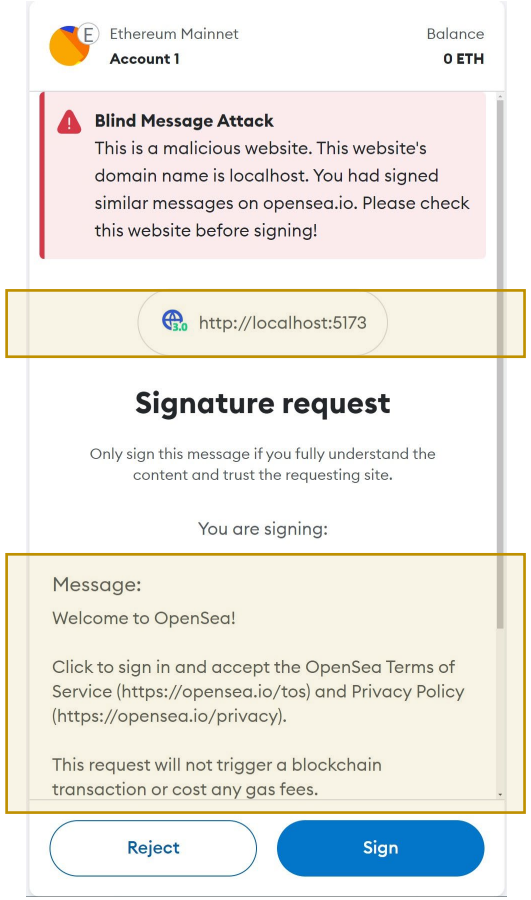
1. Record the user signed messages.
2. Extract the static fields (message body) as the template.
3. When the user logs into a new website, Web3AuthGuard performs fuzzy matching between the new message and the stored templates (messages).
4. If there is a match but the website domain is different, this is an attack.

Web3AuthGuard automatically checks the source of the message and alerts potential attacks on the crypto wallet.

Client-Side Mitigation: Web3AuthGuard

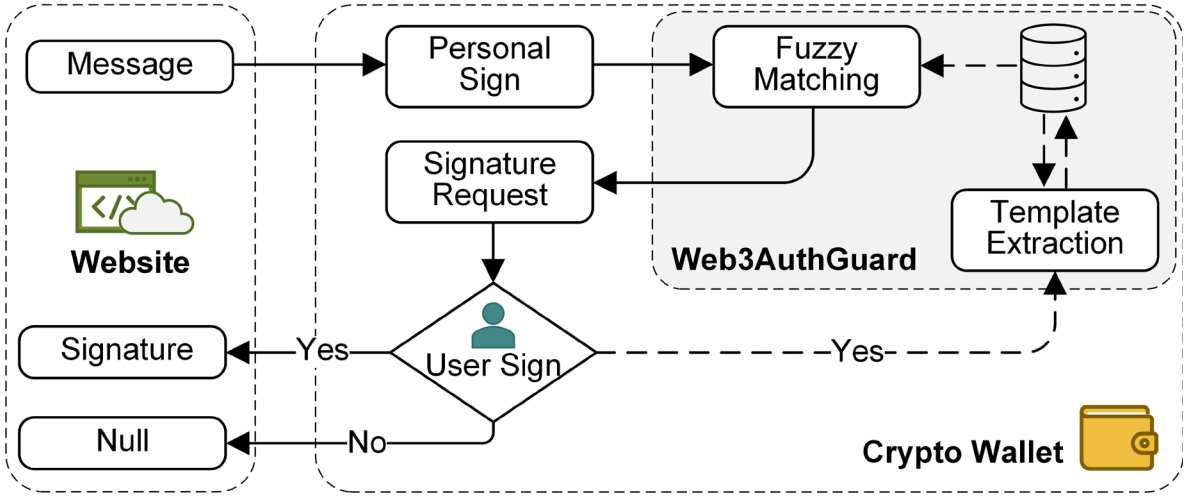


Web3AuthGuard automatically checks the source of the message and alerts potential attacks on the crypto wallet.



Blind Message Attack Alert

Client-Side Mitigation: Web3AuthGuard



Web3AuthGuard automatically checks the source of the message and alerts potential attacks on the crypto wallet.

20/25
User Login

Web3AuthGuard successfully alerted attacks in 20 out of 25 user login cases.

The remaining five cases have server-side vulnerabilities, making our client-side solution ineffective.

Summary

- Introduced the Blind Message Attack in Web3 login.
- Developed a tool Web3AuthChecker and found 75.8% websites were vulnerable.
- Proposed Web3AuthGuard, a client-side solution for immediate protection against attacks.

Kailun Yan:
kailun@mail.sdu.edu.cn

Attack Demo

CVE: CVE-2023-50053 CVE-2023-50059

Demo: https://sites.google.com/view/web3auth

Web3AuthChecker: https://github.com/d0scoo1/Web3AuthChecker

Web3AuthGuard: https://github.com/d0scoo1/Web3AuthGuard

Image generated by ChatGPT.

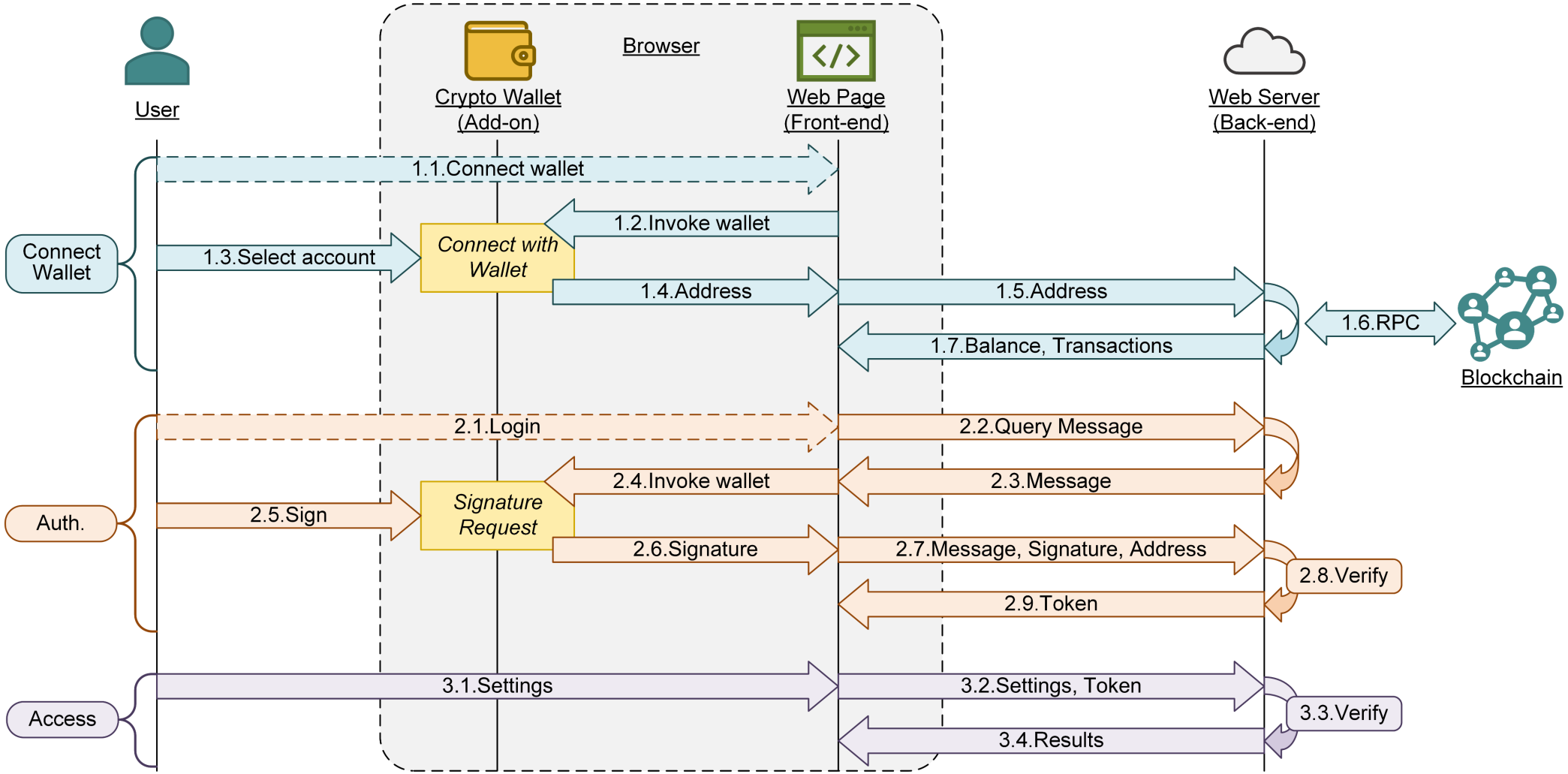
Backup Slides

- Web3 vs. Web2
- Web3 Login Workflow
- Blind Message Attack vs. Man-in-the-Middle Attack
- Mitigation: Server-side vs. Client-side Solution
- Detection: Challenges & Solutions
- Detection: Examples
- Web3AuthGuard: Alerts
- Web3AuthGuard: Templates
- EIP-4361 (Sign-with Ethereum)

Web3 vs. Web2

	Web2	Web3
Data Ownership	Controlled by centralized entities (e.g., companies, platforms)	Owned and controlled by users (via blockchain)
Architecture	Centralized servers and databases	Decentralized (blockchain-based)
Identity	Managed by third-party services (e.g., Google, Facebook login)	Managed by users themselves (public-private key pairs)
Security	Vulnerable to centralized data breaches	Enhanced security via cryptography and decentralization
Governance	Decisions made by centralized entities	Governed by users (e.g., DAOs through token voting)

Web3 Login Workflow



Blind Message Attack vs. Man-in-the-Middle Attack

Blind Message Attack

- Utilize the vulnerabilities on Web3 login
- Select the victim website

Man-in-the-Middle Attack

- Attacker intercepts communication between the client and server

Mitigation: Server-side vs. Client-side Solution

Server-side Solution

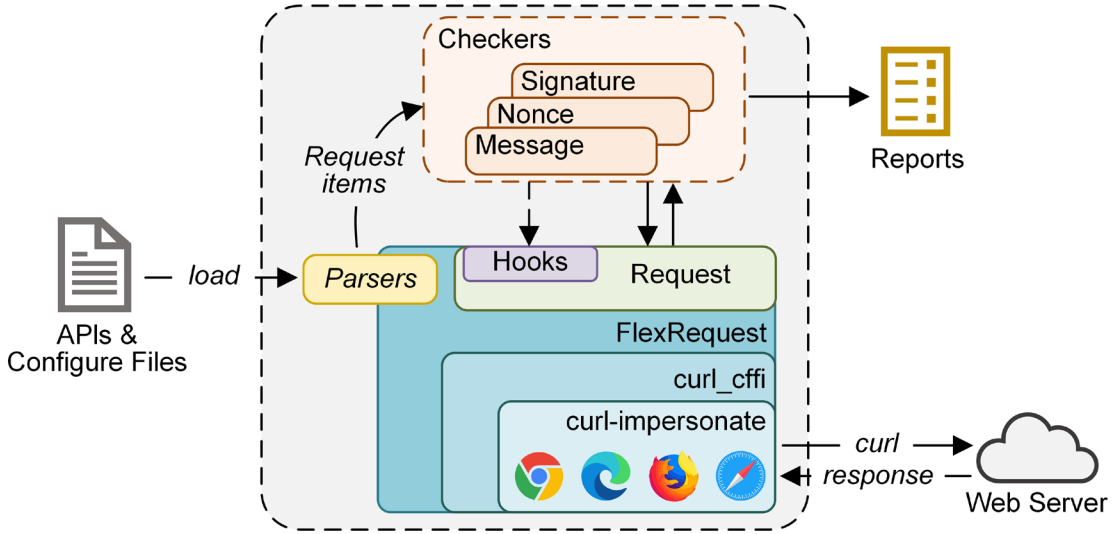
- Design a New Protocol
- Upgrade Server and Crypto Wallet
- Difficult Rollout

Client-side Solution

- Upgrade Crypto Wallet
- Simple Implementation
- Effective for Most Scenarios
- User-Activated Instantly

Detection: Challenges & Solutions

- Diverse API Implementations
  - Abstract the workflow: query, auth, access
- Dynamic Parameters
  - Key-value mechanism (Attack Payloads)
- Request Limitation
  - Curl_cffi: impersonate browsers request
- Front-End Logic
  - Web3.js mocks crypto wallet operation



Detection: Examples

```
QUERY Response:
{'data':{'auth':{'message':'This is Galler, welcome...
timestamp: 1625468800000'}}}

AUTH Request:
{method:'POST', url:'https://www.galler.io/api/v1',
headers:{...}, data:{address:'{{ addr }}',
message:'{{ msg }}', signature:'{{ sig }}'}}
```

The Response and Request of galler.io

```
msgBody: 'This is …'
nonce: None,
addr: '0x1234…'
Msg: msgBody + nonce
Sig: sign(msg, addr)
```

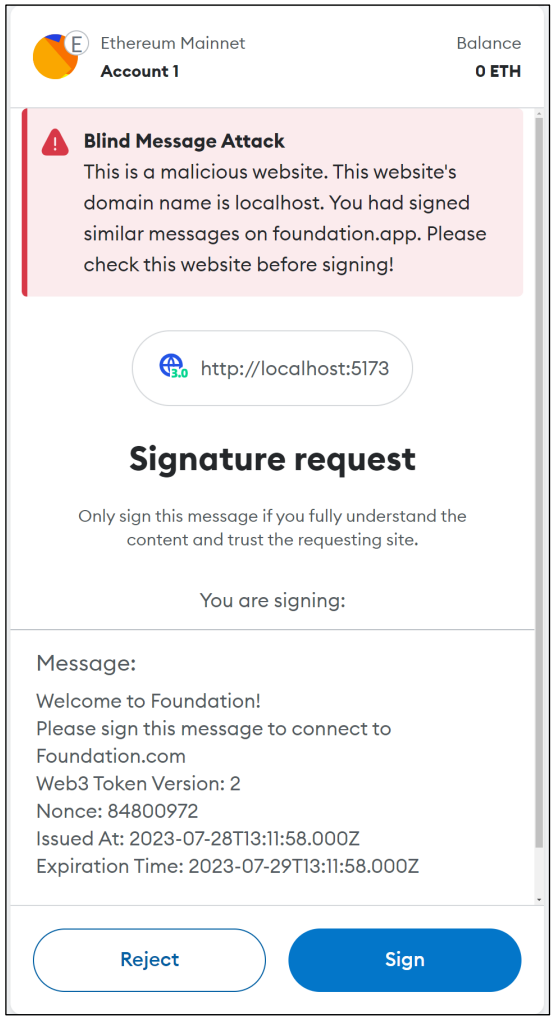
```
QUERY Response:
{'data':{'auth':{'nonce':'3deca92b'}}}

AUTH Request:
{method:'POST', url:'https://api.element.market/graphql',
headers:{'x-viewer-addr':'{{ addr }}',...}, data:{message:
'{{ msg }}', nonce:'{{ nonce }}', signature:'{{ sig }}'}}
```

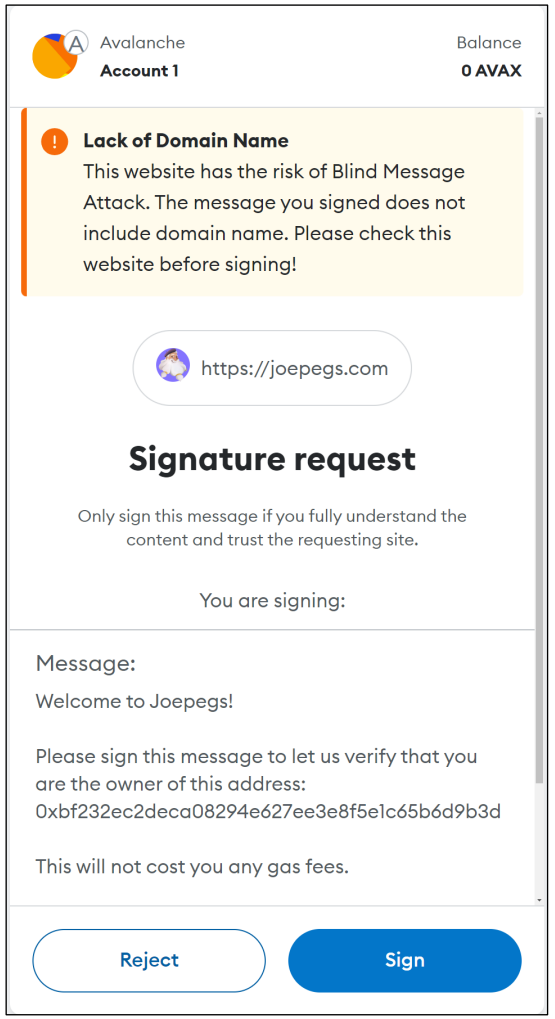
The Response and Request of element.market

```
msgBody: 'This is …'
nonce: 3deca92b,
addr: '0x1234…'
Msg: msgBody + nonce
Sig: sign(msg, addr)
```

Web3AuthGuard: Alerts

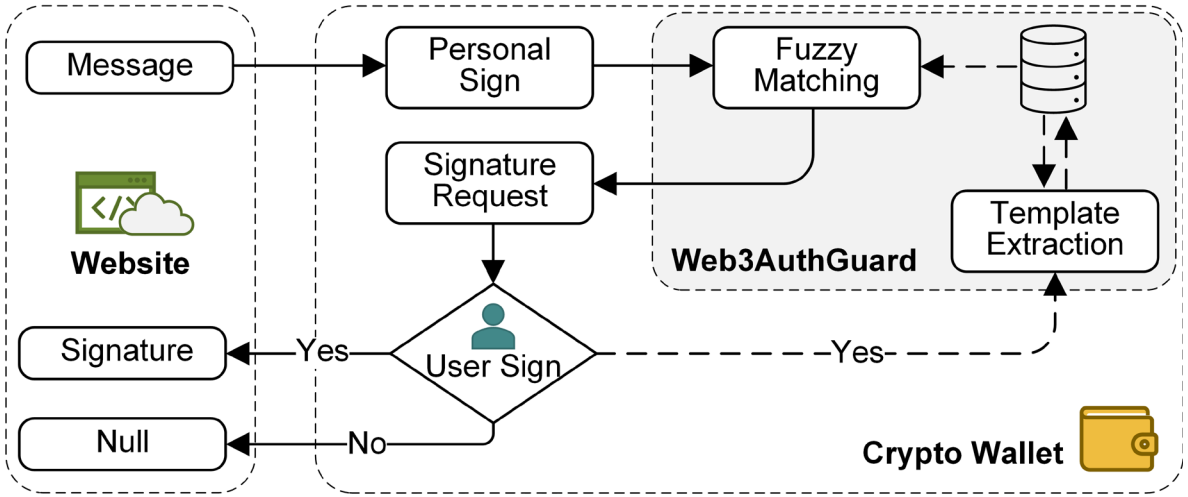


Blind Multi-Message Attack



Lack of Domain Name

Web3AuthGuard: Templates




```
Welcome to OpenSea!
This request will not trigger a blockchain transaction or
cost any gas fees.
Click to sign in and accept the OpenSea Terms of Service:
https://opensea.io/tos
Your authentication status will reset after 24 Hours.
Wallet address: 0x36e7c6feb20a90b07f63863d09cc12c4c9f39064
Nonce: 66ffb8f1-5eb1-4477-9558-36a60eb1b51f
```

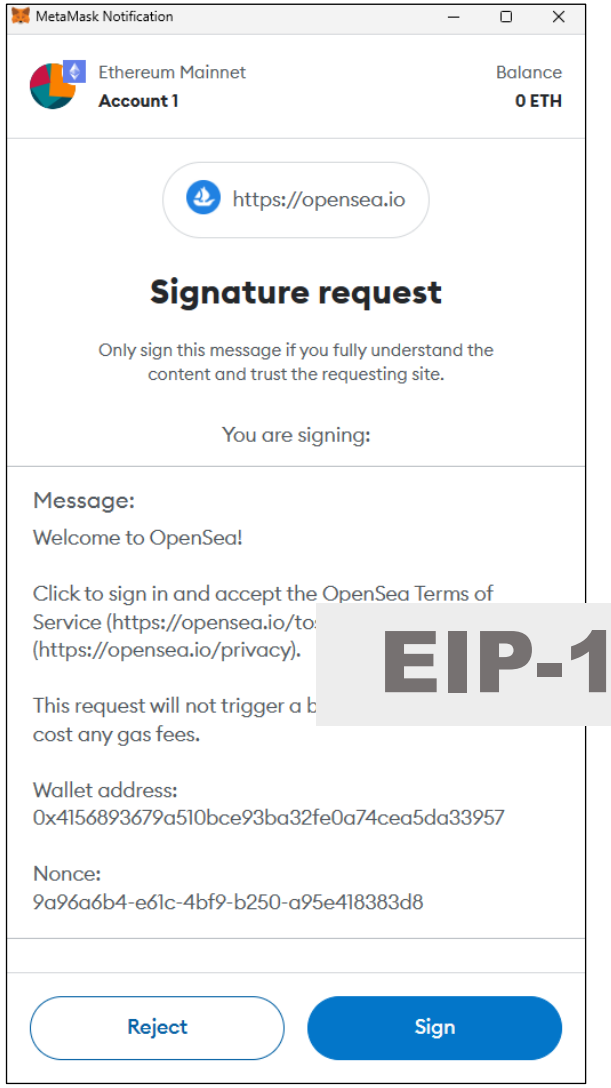
opensea.io

```
Welcome to OpenSea!
This request will not trigger a blockchain transaction or
cost any gas fees.
Click to sign in and accept the OpenSea Terms of Service:
https://opensea.io/tos
Your authentication status will reset after 24 Hours.
Wallet address: $addr$
Nonce: $nonce$
```

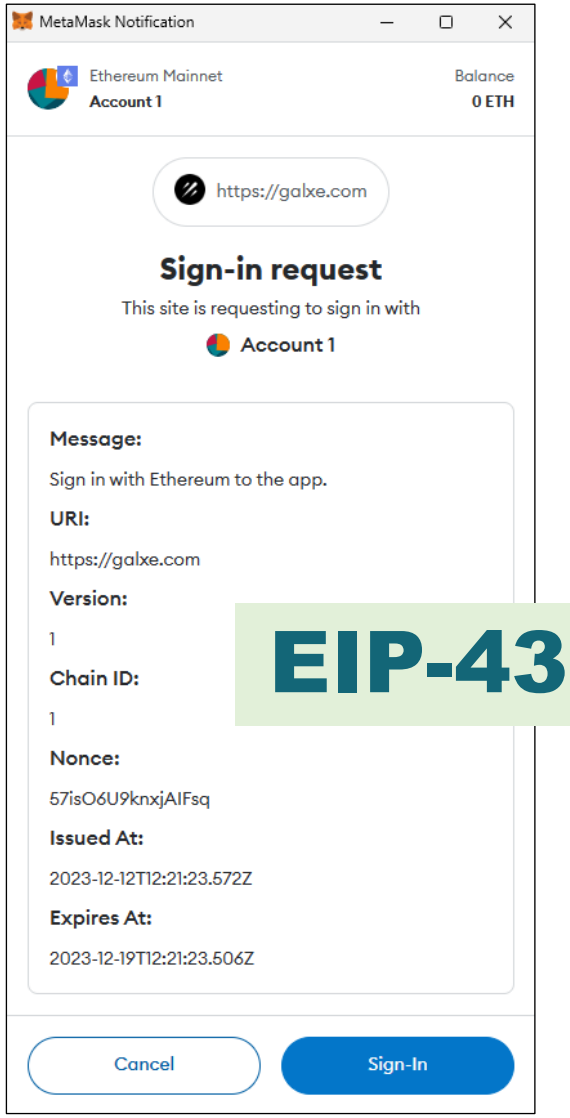
opensea.io (template)

Web3AuthGuard automatically checks the source of the message when the user signs and alerts potential attacks.

EIP-4361 (Sign-with Ethereum)



EIP-191



EIP-4361

SIGN IN WITH
ETHEREUM

2/27