Ethereum Crypto Wallets under Address Poisoning: How Usable and Secure Are They?

Shixuan Guan
sguan6@stevens.edu
Stevens Institute of Technology
Hoboken, NJ, USA

Kai Li
kli50@stevens.edu
Stevens Institute of Technology
Hoboken, NJ, USA

ABSTRACT

Blockchain address poisoning is an emerging phishing attack that crafts "similar-looking" transfer records in the victim's transaction history, which aims to deceive victims and lure them into mistakenly transferring funds to the attacker. Recent works have shown that millions of Ethereum users were targeted and lost over 100 million US dollars.

Ethereum crypto wallets, serving users in browsing transaction history and initiating transactions to transfer funds, play a central role in deploying countermeasures to mitigate the address poisoning attack. However, whether they have done so remains an open question. To fill the research void, in this paper, we design experiments to simulate address poisoning attacks and systematically evaluate the usability and security of 53 popular Ethereum crypto wallets. Our evaluation shows that there exist communication failures between 12 wallets and their transaction activity provider, which renders them unable to download the users' transaction history. Besides, our evaluation also shows that 16 wallets pose a high risk to their users due to displaying fake token phishing transfers. Moreover, our further analysis suggests that most wallets rely on transaction activity providers to filter out phishing transfers. However, their phishing detection capability varies. Finally, we found that only three wallets throw an explicit warning message when users attempt to transfer to the phishing address, implying a significant gap within the broader Ethereum crypto wallet community in protecting users from address poisoning attacks.

Overall, our work shows that more efforts are needed by the Ethereum crypto wallet developer community to achieve the highest usability and security standard. Our bug reports have been acknowledged by the developer community, who are currently developing mitigation solutions.

1 INTRODUCTION

The rapid development of the blockchain technology and the flourishing of cryptocurrency markets have brought various scams [28, 34, 37–40, 43, 44, 44, 46] and phishing attacks [24, 27, 31, 36] targeting cryptocurrency holders. Among them, address poisoning is an emerging phishing attack that typically uses "look-alike" addresses to craft phishing transfers to deceive victims, aiming to lure them into mistakenly transferring funds to the attacker. Existing works [33, 35, 42] have reported the *token-based address poisoning attack* on the Ethereum blockchain, where the attackers crafted phishing token transfers to poison victims' ERC-20 [11] token transfer history. It is shown that attackers crafted three types of phishing token transfers with the "look-alike" address: zero-value, dust-value, and fake token transfers, which caused the victims to lose over 100 million US dollars due to mistakenly transferring funds to the phishing address. More recently, it is reported that attackers also utilized new phishing strategies to attack victims by transferring the native coin, ETH, to poison their transactions history, which we refer to as *ETH-based address poisoning attack*. In this new phishing attack, attackers also crafted three types of phishing transactions: zero-ETH, dust-ETH, and fake-ETH transfers. Such an attack has caused the victim to lose more than 68 million US dollars [2].

Research statement: While the address poisoning attacks have led to such a significant financial loss to victims, it is unknown whether stakeholders in the Ethereum developer community have deployed effective countermeasures to mitigate this threat. Ethereum crypto wallets, which serve as the cornerstone for users to browse transaction history and initiate transactions to transfer funds, thereby play a central role in mitigating the threat. To fill the research gap, in this paper, we choose to measure Ethereum crypto wallets and evaluate their usability and security under the address poisoning attack. Specifically, we aim to answer the following five research questions.

- **RQ1:** Are the crypto wallets supporting users to browse their transaction activity history?
- **RQ2:** Are the crypto wallets providing good usability to users by displaying their legitimate transfers?
- **RQ3:** Are the crypto wallets providing good security to users by hiding or flagging the phishing transfers?
- **RQ4:** Who are the wallets' transaction activity providers? And how do they affect the wallets' usability and security?
- **RQ5:** Are there any preventive countermeasures on the wallets when users transfer to phishing addresses?

To answer these questions, we collect 53 popular Ethereum crypto wallets and design experiments to respectively simulate the "token-based" and "ETH-based" address poisoning attacks against them. Specifically, we first generate three Ethereum addresses and then conduct transactions involving both legitimate and phishing transfers of USDT and ETH among them. After our testing transactions are comfirmed on the Ethereum mainnet, we then launch each wallet to import the generated addresses and check if the wallet supports the display of the address's transaction activity. We define three usability levels and five risk levels to respectively quantify the wallet's usability and security under the address poisoning attack. Moreover, we also use Chrome's inspection tool and Wireshark [23] to capture the network traffic of each wallet to identify its transaction activity provider. Finally, on each wallet, we attempt to transfer funds to the phishing address involved in the address poisoning attack to evaluate if there are preventive countermeasures. All our experiments are executed in a contained environment and only affect Ethereum addresses under our control.

Research findings: Our evaluation on the 53 Ethereum crypto wallets reveals several interesting findings. First, we found that 51 out of 53 wallets provide an entry on the wallet's UI to show the users' transaction activity, while only two wallets do not (answers to **RQ1**). Second, among the 53 wallets, 32 wallets provide good usability and display both legitimate ETH and USDT transfers, and 4 wallets provide fair usability due to only displaying legitimate ETH transfers. In comparison, 17 wallets provide poor usability for not displaying any transfers, including popular wallets such as MetaMask and Crypto.com (answers to **RQ2**). Third, among the 36 wallets that display legitimate transfers, 6 of them are extremely risky for also displaying all three types of phishing transfers (risk level 4), including the popular Bybit and Core wallets. 10 wallets are highly risky for displaying fake transfers, but not all three types of phishing transfers (risk level 3), including the popular Uniswap and Phantom wallets. In contrast, there are 15 wallets that hide fake transfers. However, they are still risky due to displaying zero-value phishing transfers (risk level 2), including Rabby and Trust wallets. Another 5 wallets are less risky and only display dust-value phishing transfers (risk level 1), such as the Coinbase wallet (answers to **RQ3**). Moreover, by inspecting the network traffic, our analysis shows that most of the wallets are running their own backend services to feed the transaction activity history, and only 11 wallets are using third-party providers. Among the 9 distinct third-party providers, Etherscan [12] is the most frequently used one. Our further analysis shows that there exist communication failures between 12 wallets and their transaction activity provider, which leads them to be unable to download the transaction history and hence results in their poor usability. In addition, for those that hide one or more phishing transfers, only 10 wallets filter out the phishing transfers solely on the wallet end, while most of them rely on transaction activity providers to filter out phishing transfers. However, the phishing detection capability varies by wallets and transaction activity providers (answers to **RQ4**). Finally, when attempting to transfer funds to the phishing address, our testing result suggests that only three wallets throw a clear warning message to indicate the risk, which implies a significant security gap in the broader Ethereum crypto wallet community regarding protecting users from address poisoning attacks and safeguarding their funds (answers to **RQ5**).

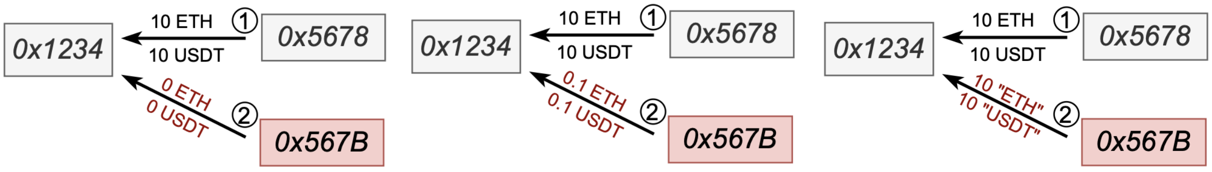
In summary, our work makes the following contributions.

- **A systematic analysis:** To our best knowledge, we are the first one that systematically evaluates Ethereum crypto wallets under the address poisoning attack by quantifying the wallet's usability and security.
- **New understandings:** Our evaluation on 53 Ethereum crypto wallets reveals several interesting findings, including that 17 wallets provide a transaction activity entry but do not display any transfers, 36 wallets are risky for displaying one or more types of phishing transfers. Moreover, we found that there exist communication failures between the wallets and the backend transaction activity providers, and most wallets are relying on the transaction activity provider to filter out phishing transfers, etc.
- **New insights:** Our work indicates that no wallet achieves the highest usability and security standard, implying that more efforts are needed by the Ethereum crypto wallet developer community. We also propose what we expect to be achieved in an ideal crypto wallet.
- **Bug report:** We have reported the usability bugs and security risks to all the affected crypto wallets. As of this writing, 11 wallets have replied, and 8 wallets have confirmed our report and discussed their mitigation plans.

2 BACKGROUND

2.1 Ethereum Crypto Wallets

Today, running a full node in the Ethereum blockchain requires a significant amount of computation and storage resources due to the ever-growing ledger size, which makes it unaffordable for average blockchain users. To relieve users' burden of running the full node themselves, various third-party services have been deployed to connect users to the Ethereum blockchain, including RPC services [3, 9, 17, 20], blockchain explorers [7, 12, 19], and crypto wallets. Among them, crypto wallets have become the primary platform utilized by users in managing their crypto assets. In general, crypto wallets can be divided into two categories:



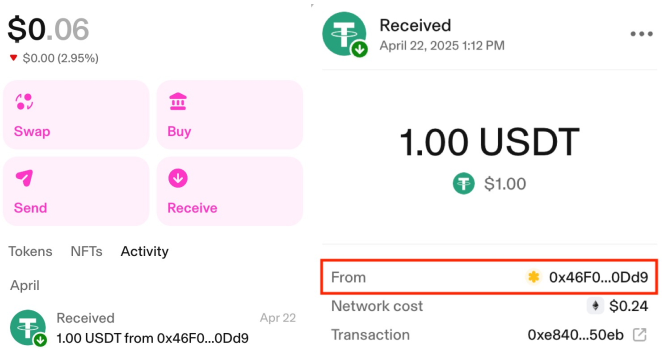
(a) Zero-value transfer. **(b) Dust-value transfer.** **(c) Fake token transfer.**

Figure 1: The workflow of Ethereum address poisoning attacks. Upon observing a legitimate transaction between two benign addresses (❶), the attacker crafts three types of phishing transactions with a similar sender address 0x567B (❷). The phishing transactions will be added to the receiver's transaction history, who may mistakenly copy the sender's address from the phishing transaction and transfer funds to it.

- **Custodial wallets** are wallets operated by a third party (such as an exchange or wallet service provider) that directly holds the user's private key. All the user's crypto assets are managed by the third-party, who will sign the transactions on the user's behalf when the payment permission is granted by the user. In this wallet model, the users must trust the third party to securely store their private keys and faithfully sign transactions on their behalf. Examples of custodial wallets provided by exchanges like Binance [5], Kraken [18], FreeWallet [15] and BitGo [6].
- **Non-custodial wallets** are wallets that offer users full control over their private keys and crypto assets, without relying on a trusted third party. In this wallet model, the responsibility of securely managing the crypto asset is solely placed on the user. Hence, the security of crypto assets depends on the user's ability to safeguard their private keys (e.g., safely store and back up the private keys). Examples include browser extension-based wallets [13], hardware wallets [16], and desktop or mobile apps [4] that allow users to directly control their private keys.

In this work, we focus on studying non-custodial wallets as the private key is directly controlled by individual users, which hence makes them the primary target of various scams and phishing attacks. Today, most non-custodial wallets are provided as browser extensions and apps, which can be installed on users' laptops or mobile devices. There are multiple functionalities provided on the wallets. For example, when launching the wallet, users can directly create a new account or import existing accounts from other sources. In addition, on the wallet's UI, users can view the balance of different crypto assets, initiate transactions to transfer the assets, and browse the past transaction activity. In Fig. 2, we show such functionalities provided by one of the most popular non-custodial wallets, Uniswap.

Address shortening: In the Ethereum blockchain, users' accounts are also called Ethereum addresses, which are represented by 40 hexadecimal characters originated from the hash of the user's public key. Due to such a long sequence, it is a common practice for crypto wallets to shorten the address when displaying it on the UI. As shown in Fig. 2, Uniswap only shows the first four characters and last four characters of the transaction sender's address, while the transaction recipient's address is not displaying.


$0.06
▼ $0.00 (2.95%)

Swap
Buy
Send
Receive

Tokens NFTs Activity

April

Received Apr 22
1.00 USDT from 0x46F0...0Dd9

Received
April 22, 2025 1:12 PM

1.00 USDT
$1.00

From 0x46F0...0Dd9
Network cost $0.24
Transaction 0xe840...50eb

Figure 2: Address shortening on Uniswap.

2.2 Ethereum Address Poisoning

Because users' addresses are shortened on the crypto wallets, they can only rely on the prefix or suffix to differentiate Ethereum addresses, which makes the address poisoning attacks possible. In such an attack, the attacker typically creates a lot of addresses and then monitors transactions recorded on the blockchain. Upon identifying a suitable legitimate transaction where the sender (or receiver) address shares a similar prefix and suffix with the one of the generated addresses ("look-alike" address), the attacker then uses the "look-alike" address to send another transaction (denoted as phishing transaction) to the receiver (or sender) of the legitimate transaction. Since both the legitimate and phishing transactions will be added to the receiver's transaction history, the receiver could be deceived by the phishing transaction and mistakenly transfer assets to the "look-alike" address, resulting in financial loss.

2.3 Address Poisoning Strategies

In general, address poisoning attacks on Ethereum can be divided into two categories: token-based address poisoning and ETH-based address poisoning. In the research community, recent works (Guan et al. [35] and Chen et.al [33]) have reported that attackers utilized "look-alike" addresses to transfer ERC-20 tokens to victims, which aims to craft a "similar-looking" token transfer record in the victim's token transfer history. We denote such "similar-looking" token transfers sent by attackers as token-based address poisoning attacks. On the social media, a recent post [2] reported that attackers also utilized "look-alike" addresses to transfer the native coin, ETH, to victims, which aims to craft a "similar-looking" transaction record in the victims' transaction history. We thereby denote the "similar-looking" ETH transfer as ETH-based address poisoning attacks. Fig. 1 shows the typical workflow of such two types of address poisoning attacks. In both attacks, the attacker can craft three types of phishing transfers to deceive victims: zero-value transfer, dust-value transfer, and fake-token transfer.

Zero-value transfer: Upon finding a legitimate transaction received by the victim in step ❶, the attacker utilizes a phishing address *0x567B* to send zero amount of valuable token or ETH to the victim's address (❷). After that, the victim *0x1234* will observe two transactions displayed on the crypto wallet: the legitimate transfer from *0x5678*, and the zero-value transfer from *0x567B*. Since such two addresses look highly similar, when the victim decides to transfer crypto assets back to the legitimate address *0x5678*, she/he may mistakenly copy the phishing address *0x567B* and transfer funds to it, resulting in financial loss.

Dust-value transfer: This phishing transfer works similarly to the above and only differs in step ❷. That is, instead of transferring zero amount, the attacker uses the phishing address to transfer a tiny amount of valuable token or ETH to the victim. Likewise, such a phishing transfer will be displayed on the victim's crypto wallets, which could mislead them to transfer funds to the phishing address, resulting in financial loss. Compared to the zero-value transfer, while dust-value transfer incurs a higher cost, it could increase the attacker's success rate as the transferred amount in the phishing transaction can be adjusted to look more similar to the transferred amount in the legitimate transaction.

Fake-token transfer: Since the transferred amount in the above two phishing transfers cannot match exactly with the amount of the legitimate transaction, an economic solution adopted by the attacker is to deploy fake ERC20 tokens or "ETH" tokens and craft phishing transfers that have the same transferred amount. After observing a legitimate transaction, the attacker then uses the phishing address *0x567B* to transfer "fake" amount to the victim address *0x1234*. Such a phishing transfer will also be displayed on the victim's crypto wallets and potentially lead them to transfer funds to the attacker.

3 ETHEREUM WALLET MEASUREMENT

As described in Sec. 2, both the token-based and ETH-based address poisoning attacks aim to poison victims' transaction history. Given the fact that crypto wallets are the primary platform utilized by cryptocurrency users in browsing transaction history and transferring funds, it is thus imperative for them to deploy countermeasures to mitigate the threat of address poisoning attacks. However, to the best of our knowledge, it remains an open question whether the crypto wallets have done so to protect their users. In this paper, we aim to answer this question by systematically testing popular Ethereum crypto wallets and evaluating their usability and security under the address poisoning attack.

3.1 Methodology

To evaluate the usability and security of Ethereum crypto wallets, we choose to download them and simulate the actual address poisoning attack against a victim address under our control. Fig. 3 shows our evaluation methodology. After installing the crypto wallet apps, we execute a testing script to send both legitimate and phishing transactions to the victim address. After the transactions are included in the Ethereum mainnet, we then launch each wallet and import the victim address to download the transaction history. Meanwhile, we use Chrome's inspection tool and Wireshark [23] to capture the wallet's network traffic. Finally, we enter the "transaction activity" entry on the wallet to check if legitimate and phishing transactions are displayed.

3.2 Measurement Process

Preparation: We begin by leveraging the public crypto wallet listing and ranking platforms CryptoSlate [10] and Alchemy [3] to collect Ethereum crypto wallets. In total, we download 53 Ethereum crypto wallets and install them on our laptop. Among them, 51 wallets are Chrome Extensions (CE), and two wallets are Desktop apps. After that, we develop a testing script to simulate the address poisoning attack with the following three externally-owned addresses (EOA).

- **V**: victim address that receives funds;
- **B**: Benign address that transfers funds to **V**;
- **P**: phishing address that looks like **B**, which will launch the address poisoning attack against **V**;

We obtain Address **V** (`0x71aF257EF2fA722694E1621B6f1D968c28Dd7A95`) by directly creating an account on the MetaMask wallet. To create the two similar addresses (**B** and **P**),

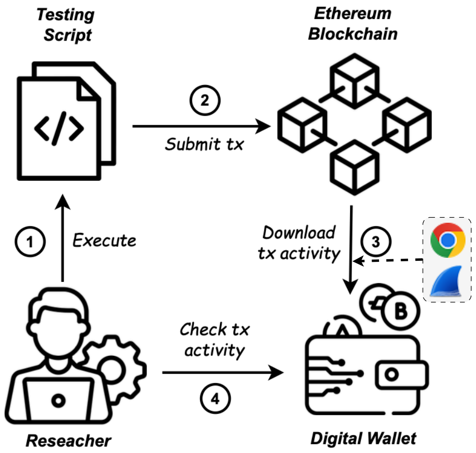


Figure 3: Our wallet evaluation methodology.

we implement a Python script to invoke the `eth_createAccount` library function to generate addresses. After executing the function more than 200K times, we obtain a suitable **B** (`0x46F0196EdBb29Bd3715E7F556c8633efDe1D0Dd9`) and **P** (`0x46F0042749ad2383471639b57833cd80bf1f0Dd9`), which share the same four characters at the beginning and ending segments. After that, we also need to identify the following three token contract addresses on the Ethereum mainnet.

- **Legit USDT contract**: to emit legit-USDT, zero-USDT, and dust-USDT transfers;
- **Fake USDT contract**: to emit fake-USDT transfers;
- **Fake "ETH" contract**: to emit fake-ETH transfers;

The legitimate USDT contract is well-known at address `0xdAC17F958D2ee523a2206206994597C13D831ec7`. For the fake USDT and ETH contracts, although we can deploy them on the Ethereum mainnet ourselves, we chose not to. Instead, we leverage the existing fake tokens already deployed by the attackers, thereby avoiding further pollution of the Ethereum mainnet. From the thousands of fake tokens flagged on Etherscan [12], we test each flagged token contract locally until we find one that allows us to send transactions to execute the `transferFrom` function with an arbitrary sender, recipient, and amount. Through testing, we found a suitable fake USDT token deployed at `0xF27d16****eA2A85` and a fake "ETH" token deployed at `0x046674****fC7445`.

Send testing transactions: After installing the crypto wallets and obtaining the addresses, we import the private key of **V** into each wallet and then execute the testing script to send transactions to transfer ETH and USDT from **B** and **P** to **V**. Two sets of transactions are sent to respectively simulate the ETH-based and token-based address poisoning attacks, each containing five transactions as shown in Table 1. TX1 simulates a legitimate ETH transfer from **B** to **V**, while TX2 - TX4 simulate zero-ETH, dust-ETH, and fake-ETH transfers from **P** to **V**. TX5 simulates a special fake-ETH transfer with zero amount. Similarly, TX6 simulates a legitimate USDT transfer, and TX7 - TX9 simulate zero-USDT, dust-USDT, and fake-USDT transfers. TX10 simulates the special fake-USDT transfer with zero amount.

Table 1: Transactions simulating the ETH-based and token-based address poisoning attacks.

TX	From	To	Amount	Transfer	Hash
1	B	V	0.001	legit ETH	0x06ae70...db8dec
2	P	V	0	zero-ETH	0x453460...92dc5c
3	P	V	0.00001	dust-ETH	0xf91b8a...97de23
4	P	V	0.001	fake-ETH	0xb0dc19...fe05cd
5	P	V	0	fake-ETH	0x61166f...551128
6	B	V	10	legit USDT	0xb4041d...5aafe7
7	P	V	0	zero-USDT	0x7c076b...c646b9
8	P	V	0.01	dust-USDT	0x93a38c...4b6892
9	P	V	10	fake-USDT	0xe3dc33...9fefa0
10	P	V	0	fake-USDT	0x5a7042...a53672

Launch the wallet app: After our testing transactions are included on the Ethereum mainnet, we launch each crypto wallet on our laptop and enter the "transaction activity" tab to observe if the testing transactions are displayed. We check the following three conditions to assess both the wallet's usability and security: **C1**: the legitimate transfers are displayed; **C2**: the phishing transfers are displayed; **C3**: the addresses in each transfer are shortened.

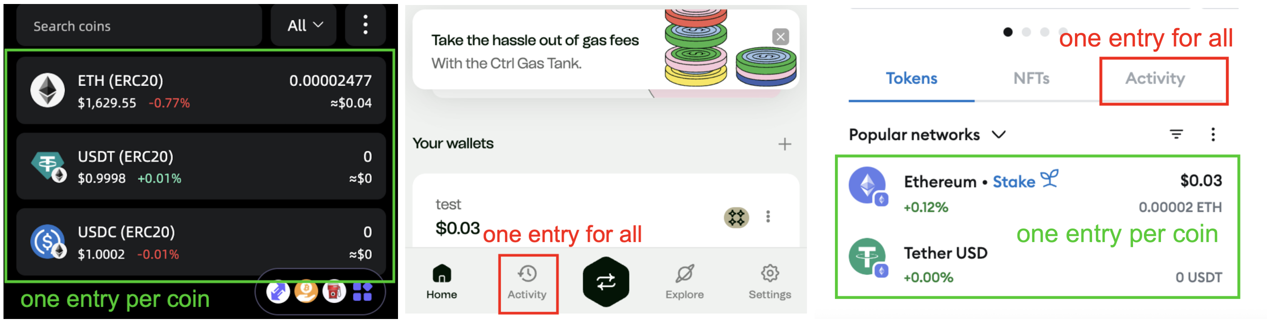
4 WALLET MEASUREMENT RESULTS

This section details our measurement results of 53 Ethereum crypto wallets, including the designs of transaction activity entry, display of legitimate and phishing transfers, transaction activity provider, and transaction warning features.

4.1 Design of Transaction Activity Entry

By launching the 53 wallets to check the transaction activity, our first observation is that several crypto wallets do not provide a UI entry to display users' transaction activity. In addition, crypto wallets that provide this functionality have different UI designs for displaying transaction activity. In Table 2, we summarize our observations.

Among the 53 crypto wallets, Frame and Cypher are the only two wallets that do not provide an entry to show users' transaction activity on the UI. For the remaining 51 wallets providing such functionality, their transaction activity entries generally have three types of designs. The first type is "one entry per coin", where the wallets separate the transaction activity by the type of crypto assets. As shown in Fig. 4a,



(a) One entry per coin (Safepal)

(b) One entry for all (Ctrl)

(c) Hybrid (MetaMask)

Figure 4: Three designs of transaction activity entry.

Table 2: Designs of transaction activity entry.

Tx Activity	Wallets
No entry	Frame, Cypher
One entry per coin	Coin98, Klever, SafePal, FoxWallet, Nabox, Tomato
One entry for all	Ctrl, Enkrypt, Frontier, Zeal, Phantom, Rabby, Rainbow, Sender, SubWallet, Uniswap, Virgo, WigWam, Zerion, Nest, Quantum Nightly, Nufi, JustLiquidity, Safnect
Hybrid	Coinbase, Bybit, Core, Backpack, Gate, Hana, Onekey, Taho, Exodus, OKX, TokenPocket, Trust, Pontem, Bitget, MetaMask, Aurox, Crypto.com, Keplr, Infinity, Nufinetes, Superhero, Wombat, Zapit

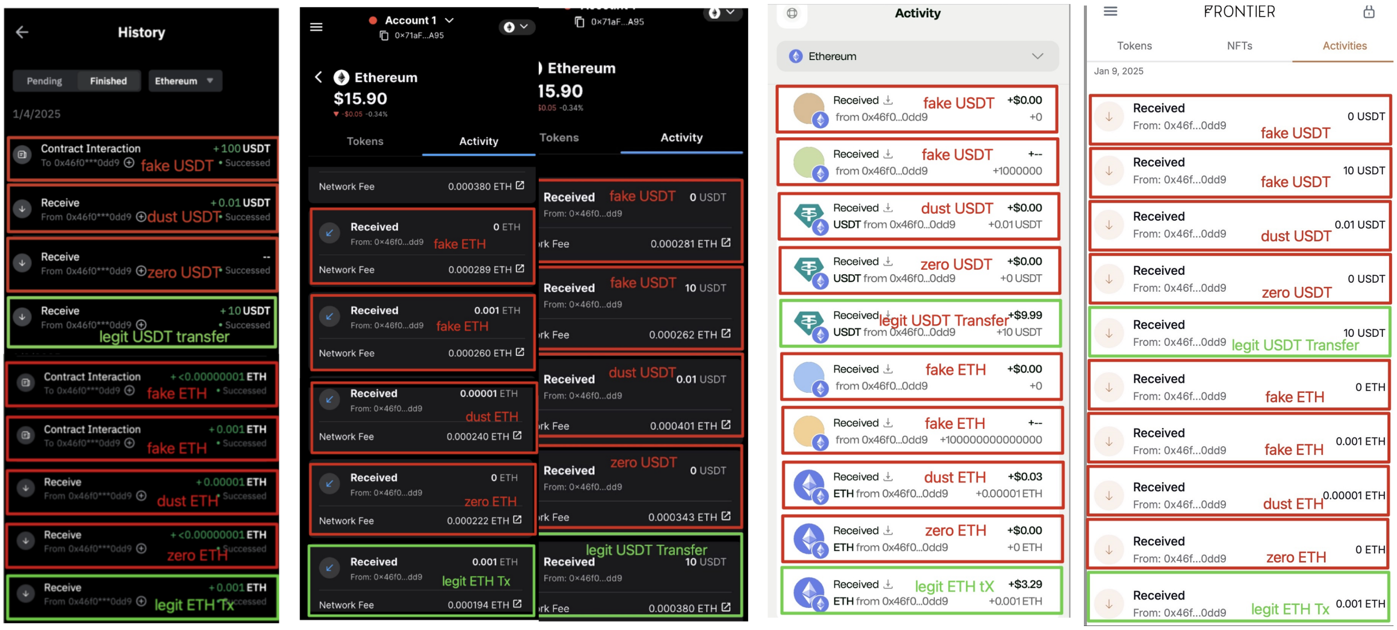
in such a design, the native coin "ETH" has its own entry for all "ETH" transfers, and each popular ERC-20 tokens, such as USDT and USDC, also have its own entry to show the corresponding transaction activity. Users can also manually create a new entry to add other tokens. Our observation shows that 6 wallets, including Klever, Safepal, and FoxWallet, etc, employed such a design. The second type is "one entry for all", where the wallets simply merge all transfers into one entry, regardless of the type of crypto assets, as shown in Fig. 4b. In this design, users cannot manually create an entry for a specific token. Our result indicates that 19 wallets, such as Ctrl, Phantom, Uniswap, Zerion, Nightly, etc, adopted such a design. The last type is a hybrid design that supports both "one entry per coin" and "one entry for all". It thus depends on the users' preference to select an entry to browse the transaction activity. Fig. 4c shows an example of such a hybrid design. Our observation suggests that 23 wallets have employed a hybrid design, including Coinbase, Backpack, Trust, MetaMask, Crypto.com, etc.

4.2 Display of Legitimate Transfers

We assess each wallet's usability by checking condition **C1**: display of legitimate transfers. Since there are two types of legitimate transfers (ETH and USDT) that could be displayed in the transaction activity entries, we define the following criteria to quantify the usability. The higher the level is, the better usability the wallet can provide. For wallets employing a hybrid design of the transaction activity entry, we enter all possible entries to assign the usability level.

- **Level 2**: display legitimate ETH and USDT transfers;
- **Level 1**: display only one legitimate transfer;
- **Level 0**: display none of the legitimate transfers;

Findings: Our measurement result shows that 17 wallets do not display any transfers, including Frame, 1chainAi, Crypto.com, MetaMask, Nightly, SubWallet, as listed in Table 3. Due to this, their usability level is 0. It is also unknown whether they would shorten the user's address. All the remaining 36 wallets display the legitimate transfers, as shown in Table 4. Among them, 4 wallets provide usability at level 1 due to only displaying the legitimate ETH transfer, such as Enkrypt, FoxWallet, Klever, and Pontem. The other 32 wallets provide usability at level 2 for displaying both legitimate ETH and USDT transfers. It is also interesting to see that no wallets would only display the legitimate USDT transfer without showing the legitimate ETH transfer, which implies that displaying ETH transfers has a higher priority than token transfers. This can be explained by the fact that ETH is the fiat currency on Ethereum, and ETH transfers are more frequent than token transfers. Besides, when transferring tokens, users must have ETH in their accounts to pay the transaction fee. Due to these reasons, supporting ETH transfer history has a higher priority than token transfer history in the design of Ethereum crypto wallets.



(a) Bybit (b) Core (c) Ctrl (d) Frontier

Figure 5: Transfers displayed by four extremely risky wallets (risk level=4).

Table 3: 17 wallets that do not display any transfers. "CE" indicates the wallet is a Chrome Extension.

Wallet	Type	Usability Level	Risk Level
Frame	Desktop	0	0
1chainAi, Aurox, Arcana, Crypto.com, Cypher, Fluvi, Keplr, JustLiquidity, MetaMask, Nabox, Nightly, Nufinetes, Quantum, SubWallet,Virgo, Zapit	CE	0	0

4.3 Display of Phishing Transfers

When condition **C1** is satisfied, we assess the crypto wallets' security using condition **C2**: display of phishing transfers, and condition **C3**: addresses are shortened. To quantify the risk, we define the following five risk levels and assign one of them to each tested wallet if the associated requirement is satisfied. The higher the level is, the more risky the wallet is.

- **Level 4**: display all phishing transfers;
- **Level 3**: display fake-ETH or fake-USDT transfers;
- **Level 2**: display zero-ETH or zero-USDT, or conditionally display fake transfers[1];
- **Level 1**: display dust-ETH or dust-USDT transfers;
- **Level 0**: display none of the phishing transfers;

In the above definition, we consider level 4 extremely risky because all three types of phishing transfers are displayed, which thus poses the highest risk to the wallet user. We consider level 3 highly risky because, compared to zero-value and dust-value transfers, fake transfers can be crafted at a lower cost while looking highly similar to the legitimate transfer, hence posing a higher risk to the wallet user. Level 2 is considered less risky since zero-value transfers and conditionally displayed fake transfers will not look highly similar to legitimate transfers. For level 1, we consider displaying dust-value transfers less risky than level 2 because dust-value transfers incur a higher attack cost than zero-value transfers.

Findings: Since the 17 wallets in Table 3 do not satisfy **C1** and display no transfers, their risk level is thus 0. For the remaining 36 wallets listed in Table 4, they all shorten users' addresses. Among them, 6 wallets, such as Bybit, Core, Ctrl, and Frontier, display all three types of phishing transfers, which hence have the highest risk level (level 4: extremely risky). In addition, there are 10 wallets, such as Backpack, Gate, Hana, OneKey, Phantom, Taho, Uniswap, and Zeal, displaying either fake-ETH or fake-USDT transfers, but not all three types of phishing transfers. Hence, their risk level is assigned to 3 (highly risky). Moreover, there are 15 wallets displaying zero-ETH or zero-USDT transfers but not fake transfers, such as Coin98, Enkrypt, Exodus, Rabby, and Trust etc. Hence, their risk level is lower, which is assigned to 2. Finally, 5 wallets are assigned at risk level 1 due to only

[1] for example, displaying the fake transfer as a contract interaction or only displaying the special fake transfer of 0 amount.

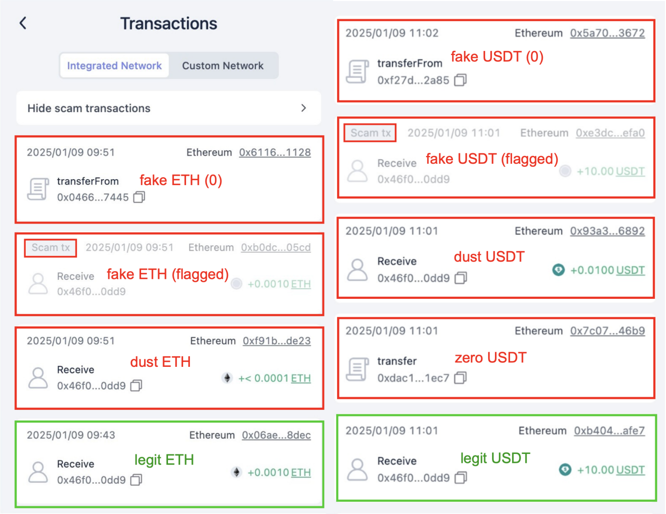
Table 4: Measurement results of 36 Ethereum crypto wallets that display transfers. ✓ indicates the transfer is displayed. ✗ indicates the transfer is not displayed. ✓̸indicates the fake transfer is conditionally displayed.

Wallet	Type	ETH Transfers				USDT Transfers				Address	Usability	Risk
		Legit	Zero	Dust	Fake	Legit	Zero	Dust	Fake	Shorten	Level	Level
Bybit	CE	✓	✓	✓	✓	✓	✓	✓	✓	✓	2	4
Core	CE	✓	✓	✓	✓	✓	✓	✓	✓	✓	2	4
Ctrl	CE	✓	✓	✓	✓	✓	✓	✓	✓	✓	2	4
Frontier	CE	✓	✓	✓	✓	✓	✓	✓	✓	✓	2	4
Safnect	CE	✓	✓	✓	✓	✓	✓	✓	✓	✓	2	4
Superhero	CE	✓	✓	✓	✓	✓	✓	✓	✓	✓	2	4
Backpack	CE	✓	✗	✓	✓	✓	✗	✓	✓	✓	2	3
Gate	CE	✓	✗	✓	✓	✓	✗	✓	✓	✓	2	3
Hana	CE	✓	✗	✓	✓	✓	✓	✓	✓	✓	2	3
OneKey	CE	✓	✓	✓	✓	✓	✓	✓	✗	✓	2	3
Nest	CE	✓	✓	✓	✗	✓	✗	✓	✓	✓	2	3
Nufi	CE	✓	✗	✓	✓	✓	✗	✓	✓	✓	2	3
Phantom	CE	✓	✓	✓	✓	✓	✓	✓	✗	✓	2	3
Taho	CE	✓	✓	✓	✓	✓	✗	✓	✓	✓	2	3
Uniswap	CE	✓	✓	✓	✓	✓	✗	✓	✓	✓	2	3
Zeal	CE	✓	✗	✓	✓	✓	✓	✓	✓	✓	2	3
Coin98	CE	✓	✓	✓	✓̸	✓	✗	✓	✓̸	✓	2	2
Exodus	CE	✓	✓	✓	✗	✓	✗	✓	✗	✓	2	2
OKX	CE	✓	✓	✓	✓̸	✓	✓	✓	✓̸	✓	2	2
Rabby	CE	✓	✗	✓	✓̸	✓	✓	✓	✓̸	✓	2	2
Rainbow	CE	✓	✓	✓	✗	✓	✗	✓	✗	✓	2	2
Sender	CE	✓	✓	✓	✓̸	✓	✓	✓	✗	✓	2	2
Trust	CE	✓	✓	✓	✗	✓	✗	✓	✗	✓	2	2
TokenPocket	CE	✓	✓	✓	✗	✓	✗	✓	✗	✓	2	2
Tomato	CE	✓	✓	✓	✗	✓	✓	✓	✗	✓	2	2
Wombat	CE	✓	✗	✓	✗	✓	✓	✓	✗	✓	2	2
Zerion	CE	✓	✓	✓	✗	✓	✗	✓	✗	✓	2	2
Enkrypt	CE	✓	✓	✓	✗	✗	✗	✗	✗	✓	1	2
FoxWallet	CE	✗	✓	✓	✗	✗	✗	✗	✗	✓	1	2
Klever	CE	✓	✓	✓	✗	✗	✗	✗	✗	✓	1	2
Pontem	CE	✓	✓	✓	✗	✗	✗	✗	✗	✓	1	2
Bitget	CE	✓	✗	✓	✗	✓	✗	✓	✗	✓	2	1
Coinbase	CE	✓	✗	✓	✗	✓	✓	✗	✗	✓	2	1
Infinity	Desktop	✓	✗	✓	✗	✓	✗	✓	✗	✓	2	1
SafePal	CE	✓	✗	✓	✗	✓	✗	✓	✗	✓	2	1
WigWam	CE	✓	✗	✓	✗	✓	✗	✓	✗	✓	2	1

displaying the dust-ETH or dust-USDT transfers, including Bitget, Coinbase, etc. In Fig. 5, we show the screenshots of the displayed transfers on 4 extremely risky wallets: Bybit, Core, Ctrl, and Frontier. The screenshots of other wallets are deferred to Appendix B due to page limit.

Notable effort by Rabby: In our results, it is worth mentioning that Rabby is the only one who flags phishing transfers. As shown in Fig. 6, both the fake ETH and USDT transfers are flagged as scam transactions. We hence give Rabby some credit for making such an effort in flagging phishing transfers sent by address poisoning attackers. However, our evaluation still suggests that more efforts are needed by

Rabby, as dust-value transfers and the special fake transfers with 0 amount are not flagged yet.



Transactions

Integrated Network | Custom Network

Hide scam transactions

2025/01/09 09:51 Ethereum 0x6116...1128
transferFrom 0x0466...7445
fake ETH (0)

Scam tx 2025/01/09 09:51 Ethereum 0xb0dc...05cd
Receive 0x46f0...0dd9 +0.0010 ETH
fake ETH (flagged)

2025/01/09 09:51 Ethereum 0xf91b...de23
Receive 0x46f0...0dd9 +< 0.0001 ETH
dust ETH

2025/01/09 09:43 Ethereum 0x06ae...8dec
Receive 0x46f0...0dd9 +0.0010 ETH
legit ETH

2025/01/09 11:02 Ethereum 0x5a70...3672
transferFrom 0xf27d...2a85
fake USDT (0)

Scam tx 2025/01/09 11:01 Ethereum 0xe3dc...efa0
Receive 0x46f0...0dd9 +10.00 USDT
fake USDT (flagged)

2025/01/09 11:01 Ethereum 0x93a3...6892
Receive 0x46f0...0dd9 +0.0100 USDT
dust USDT

2025/01/09 11:01 Ethereum 0x7c07...46b9
transfer 0xdac1...1ec7
zero USDT

2025/01/09 11:01 Ethereum 0xb404...afe7
Receive 0x46f0...0dd9 +10.00 USDT
legit USDT

Figure 6: Transfers displayed on Rabby

4.4 Transaction Activity Provider

Since both the wallets' usability and security are determined by the transfers displayed in the transaction activity entry, it is important to understand where and how the wallets obtain the users' transaction history. In fact, all crypto wallets rely on a backend service, which is synchronized with the Ethereum blockchain, to feed the users' transaction history. In this section, we choose to measure the backend services utilized by each crypto wallet. To achieve the goal, we leverage Chrome's inspection tool and Wireshark [23] to capture the network traffic of each wallet and analyze the HTTP requests and responses. After that, we manually inspect each HTTP response to identify the backend URL that provides wallets with the transaction history. After identifying the backend URL queried by the wallet for downloading the transaction history, we then query whois [22] to determine the entity that owns the domain name.

Entity of provider: In Table 5 and 6, we summarize the entity and domain name of the transaction activity providers used by the wallets. In addition, if the domain name is registered by the same entity operating the crypto wallet, the entity is presented as "Self". Otherwise, the entity is presented as either the third-party provider's name or "Unknown", depending on whether the registrar information is linkable to a known organization. Table 5 and 6 respectively show the transaction activity providers of 12 wallets at usability level 0 and 30 wallets at usability level > 0. We are unable to identify the provider's URL of 5 wallets in Table 5 and 6 wallets in Table 6 due to that they use the TLS communication protocol, including Arcana, Cypher, Frame, Frontier, Rainbow, FoxWallet, etc. Nevertheless, from both tables, we can see that the majority of the crypto wallets are running their own backend services to feed users' transaction history. 11 wallets are using third-party providers, such as Crypto.com, Fluvi, Nabox, Virgo, Superhero, Taho, Zeal, Coin98, Wombat, Enkrypt, and Wigwam. There is a total of 9 unique third-party providers, including Allnodes, Ankr, Publicnode, Base, Etherscan, Alchemy, AWS, Blockscount, and Infura. Among them, the most popular provider is Etherscan, which serves 3 wallets. There are another 5 wallets using a transaction activity provider from an unknown/unlinkable entity, such as 1chainAi, Nightly, SubWallet, Trust, and Bitget.

Impact on usability: For the 12 wallets in Table 5 at usability level 0, we examine the reason why they do not display any transfers. Specifically, we want to investigate whether the problem is caused by the transaction activity provider or the wallet itself. To answer this question, we manually analyze the payload of the captured HTTP packets between the wallet and the transaction activity provider. The HTTP response of each provider is summarized in Table 5. We can see that 9 wallets receive an HTTP response from their provider with a status code of 200. However, 8 of them receive empty data in the HTTP body. Ankr, the provider of the wallet Fluvi, is the only one that indicates errors in the wallet's HTTP request: "invalid API key". For the other 3 wallets, 1chainAi receives a reply of 404 from its provider, and Aurox and Virgo receive a reply of 403 from their provider. Overall, our analysis indicates that miscommunication with the transaction provider is the culprit for causing the 12 wallets not to display any transfers. To successfully retrieve users' transaction history, the wallets should either fix the errors in their requests or ask their provider to fix the errors in the response.

Impact on security: For the 30 wallets in Table 6 at usability level > 0, five wallets display all three types of phishing transfers (risk level = 4), which means that their transaction activity providers do not filter out any phishing transfers. For the other 25 wallets that hide one or more phishing transfers (risk level < 4), it is interesting to see whether the phishing transfers are filtered out by the transaction activity provider or the wallet itself. Likewise, we answer this question by manually analyzing the payload of the captured HTTP packets between the wallet and the transaction activity provider. Our analysis result is summarized in Table 6. It can be seen that for the 10 wallets at risk level 3 (from Backpack to Zeal), 8 of them have the phishing transfers filtered out by their provider, 2 of them have the phishing transfers filtered out by the wallet itself. Among them, 7 wallets filter out only zero-value transfers (zero-ETH and zero-USDT), and three wallets filter out only one of the two fake transfers (fake-USDT and fake-ETH). Besides, for the 11 wallets at risk level

Table 5: Transaction activity provider of 17 wallets that do not display transfers (usability level = 0).

Wallet	Entity	Domain Name	HTTP Response
1chainAi	Unknown	https://api.chatgm.com	404 (Not Found)
Aurox	Self	https://api.blockchain.getaurox.com	403 (Forbidden)
Crypto.com	Allnodes	https://ethereum-rpc.publicnode.com	200 (Empty body)
Fluvi	Ankr	https://rpc.ankr.com/	200 (Invalid API key)
Keplr	Self	https://evm-1.keplr.app	200 (Empty body)
MetaMask	Self	https://accounts.api.cx.metamask.io	200 (Empty body)
Nabox	Publicnode	https://ethereum.publicnode.com/	200 (Empty body)
Nightly	Unknown	https://mainnet.storyrpc.io/	200 (Empty body)
Nufinetes	Self	https://api-common.nufinetes.com	200 (Empty body)
SubWallet	Unknown	https://mainnet.storyrpc.io	200 (Empty body)
Virgo	Base	https://mainnet.base.org	403 (Forbidden)
Zapit	Self	https://gateway.zapit.io	200 (Empty body)
Arcana, Cypher, Frame, Quantum, JustLiquidity	N/A		

2 (from Coin98 to Pontem), 3 wallets filter out phishing transfers solely on the wallet end, 5 wallets filter out phishing transfers solely on the provider end, and 3 wallets filter them out collaboratively on both the provider and wallet ends. Among them, the providers of wallet Enkrypt, Klever, and Pontem have the strongest impact for filtering out all kinds of USDT transfers, including the legitimate ones. For the last four wallets at risk level 1 (from Bitget to Wigwam), two wallets have the zero-value transfers and fake transfers filtered out solely by their provider, and the other two wallets filter out zero-value and fake transfers jointly on the provider and wallet ends. Overall, our analysis indicates that most wallets rely on their transaction provider to detect and filter out phishing transfers. Some wallets choose to detect phishing transfers themselves directly on the wallet end. In contrast, only a small fraction of wallets detect phishing transfers jointly on the provider and wallet ends. However, the capability of detecting phishing transfers varies by provider and wallet. Among them, the providers of wallet Bitget and Wigwam have the strongest detection capability, and wallet TokenPocket has the strongest detection capability.

Misuse of Etherscan's API: It is also worth mentioning that wallet Superhero, Coin98, and Wombat all use Etherscan as the transaction activity provider. However, Superhero displays all three types of phishing transfers, while Coin98 and Wombat have fake transfers filtered out by Etherscan. Our investigation indicates that this is because Coin98 and Wombat both specify the legitimate USDT token's address in the request (e.g., through a parameter of "&contract_address"), but Superhero does not, which thus causes Etherscan to return both fake-ETH and fake-USDT transfers.

4.5 Transaction Warning Features

Since the ultimate goal of the address poisoning attack is to lure victims into transferring funds to the phishing address, it is thus crucial for the wallets to prevent users from interacting with phishing addresses involved in address poisoning or at least warn users about the potential risk. To evaluate whether crypto wallets have employed such a preventive or warning feature, we test each wallet by initiating transactions to transfer funds to the phishing address. Specifically, on each wallet, we initiate transactions to attempt to transfer both ETH and USDT from the victim address **V** to the phishing address **A** that we generated in the previous experiment. Since address **A** (`0x46f0042749ad2383471639b57833cd80bf1f0dd9`) has not been flagged on Etherscan, for comparison, we also initiate transactions to transfer funds to the notorious phishing address **F** (`0xa7Bf487***E90570`) that stolen 20 million USDT from Binance [1] through the address poisoning attack, which has been flagged on Etherscan. Before signing the transaction on each wallet, we check whether there are warning messages displayed or preventive measures that alert us about the potential risk.

Our testing results are summarized in Table 7. Among the 53 tested wallets, we found that 11 wallets employed different transaction warning features. Specifically, when we intend to transfer to the flagged phishing address **F**, three wallets, Bybit, Ctrl, and OKX, display a clear message warning that our transaction is highly risky, as shown in Fig. 7a. However, no warning is given when we transfer to phishing address **A**, except OKX, which reminds us that **A** is an unknown address. Besides, when we transfer to both **A** and **F** on the other four wallets, OneKey, Phantom, Rabby, and Uniswap, a transaction confirmation window is popped up, which indicates that the recipient address is unknown (e.g.,

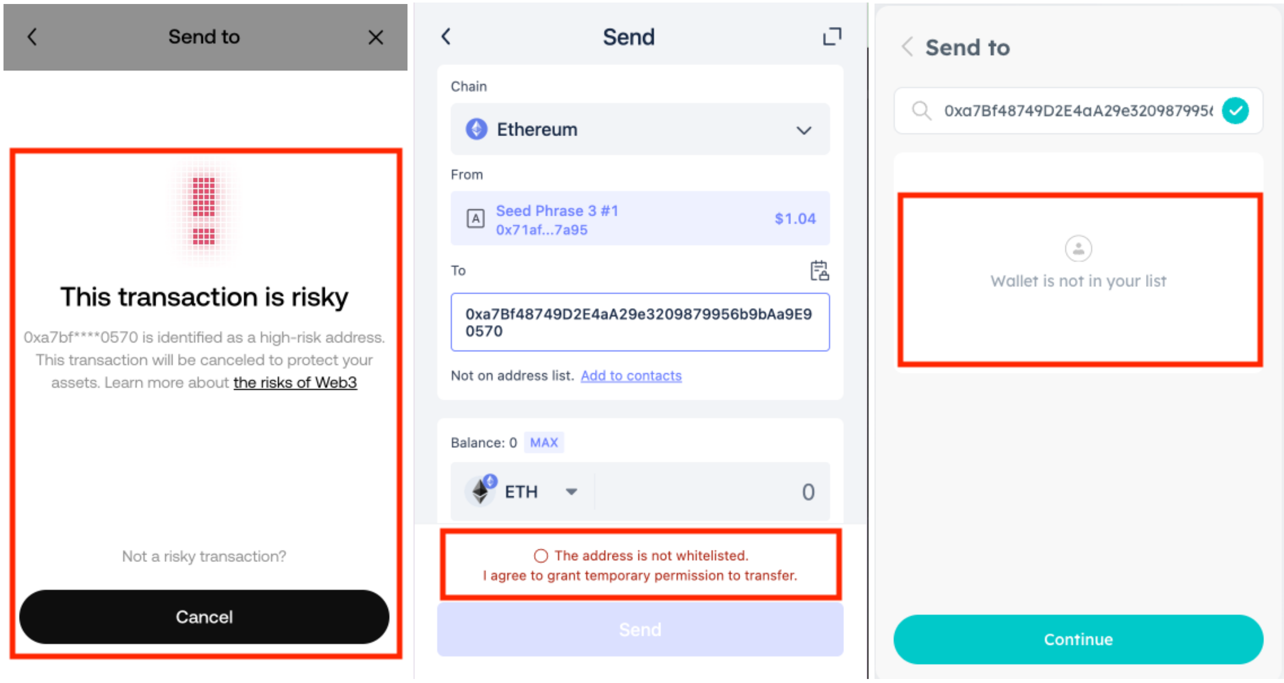
Table 6: Transaction activity provider of 36 wallets that display transfers (usability level > 0). "ZE", "FE" respectively stand for "zero-ETH", "fake-ETH" transfers. "ZU", "DU", "FU" respectively stand for "zero-USDT", "dust-USDT", "fake-USDT" transfers. "LU" stands for "legit-USDT" transfer.

Wallet	Transaction Activity Provider		Filtered by Provider	Filtered by Wallet
	Entity	Domain Name		
Bybit	Self	https://api2.bybit.com	-	-
Core	Self	https://proxy-api.avax.network	-	-
Ctrl	Self	https://gql-router.xdefi.services	-	-
Safnect	Self	https://server.safnect.com	-	-
Superhero	Etherscan	https://api.etherscan.io	-	-
Backpack	Self	https://backpack-api.xnfts.dev	ZE, ZU	-
Gate	Self	https://dapp.gateio.services	ZE, ZU	-
Hana	Self	https://api.hanawallet.io	ZE	-
Onekey	Self	https://wallet.onekeycn.com	FU	-
Nest	Self	https://api.nestwallet.app	-	FE, ZU
Nufi	Self	https://alchemy-evm.nu.fi	-	ZE, ZU
Phantom	Self	https://api.phantom.app	FU	-
Taho	Alchemy	https://eth-mainnet.alchemyapi.io	ZU	-
Uniswap	Self	https://gateway.uniswap.org	ZU	-
Zeal	Amazon AWS	https://eu-west-1.amazonaws.com	ZE	-
Coin98	Etherscan	https://api.etherscan.io	-	FE, FU, ZU
Exodus	Self	https://avax-c.a.exodus.io	FE, ZU, FU	-
OKX	Self	https://wallet.okex.org		FE, FU
Rabby	Self	https://api.rabby.io	ZE	FE, FU
Sender	Self	https://api.nearblocks.io	FU	FE
Trust	Unknown	https://ethereum.twnodes.com	FE, ZU, FU	-
TokenPocket	Self	https://pretxs.mytokenpocket.vip	-	FE, FU, ZU
Wombat	Etherscan	https://api.etherscan.io	FE, FU	ZE
Enkrypt	Blockscout	https://eth.blockscout.com	FE, LU, ZU, DU, FU	-
Klever	Self	https://apis.klever.io	FE, LU, ZU, DU, FU	-
Pontem	Self	https://control.pontem.network	FE, LU, ZU, DU, FU	-
Bitget	Unknown	https://api-app-fast.chainnear.com	ZE, FE, ZU, FU	-
Coinbase	Self	https://blockchain.wallet.coinbase.com	ZE, DU	FE, FU
Safepal	Self	https://ap.isafepal.com	FE, ZU, FU	ZE
Wigwam	Infura	https://mainnet.infura.io	ZE, FE, ZU, FU	-
Frontier, Rainbow, Tomato, FoxWallet, Infinity, Zerion	N/A			

Table 7: Transaction Warning Results

Wallet	ETH Recipient		USDT Recipient	
	A	F	A	F
Bybit	-	Alert	-	Alert
Ctrl	-	Alert	-	Alert
OKX	Reminder	Alert	Reminder	Alert
Onekey, Phantom, Rabby, Uniswap	Confirmation required			
Arcana, Nest, Quantum, Zeal	Reminder			

not in the contact list, had no prior interactions). To close the window and proceed with the transfer, we need to click the confirmation button. In Fig. 7b, we show such a transaction confirmation feature. In addition, there are another four wallets, Zeal, Arcana, Nest, and Quantum, that display a warning message showing the recipient **A** and **F** are unknown addresses (e.g., not in contact list), as can be seen in Fig. 7c. However, no confirmation is required to proceed with the transfer. In comparison, all the remaining 42 wallets do not have any forms of transaction warning or preventive measures employed when we attempt to transfer to **A** and **F**.



This transaction is risky

0xa7bf****0570 is identified as a high-risk address. This transaction will be canceled to protect your assets. Learn more about the risks of Web3

Not a risky transaction?

0xa7Bf48749D2E4aA29e3209879956b9bAa9E9 0570

Not on address list. Add to contacts

The address is not whitelisted.
I agree to grant temporary permission to transfer.

0xa7Bf48749D2E4aA29e320987995(

Wallet is not in your list

(a) Alert of high-risky address (OKX) **(b) Confirmation required when transferring to an unknown address (Rabby)** **(c) Reminder of tranferring to an unknown address (Zeal)**

Figure 7: Three types of transaction warning features when transferring to a phishing address.

In summary, our evaluation results suggest that transaction warning has not become a common feature in the design of Ethereum crypto wallets, as only three wallets, Bybit, Ctrl, and OKX, display a clear warning message when we attempt to transfer to the phishing address. This highlights a significant security gap in most crypto wallets regarding users' fund protection. While there are some wallets supporting transaction confirmation features, they simply remind us that the recipient address is unknown without explicitly informing us that we are interacting with phishing addresses. Finally, we give credit to the three wallets, Bybit, Ctrl, and OKX, that explicitly alert us about the phishing risk, which is a good preventive countermeasure. However, such an alert is only triggered when the recipient address has already been flagged. Hence, future improvements are needed for them to alert users about the risk of interacting with phishing addresses that have not been flagged.

5 DISCUSSION

Overall, our analysis suggests that among the 53 Ethereum crypto wallets, 17 wallets cannot successfully display the users' transaction history, most of which are caused by communication failures with their transaction activity provider. Among the 36 wallets that successfully display transaction history, 16 wallets cannot distinguish fake transfers from legitimate transfers, which thus pose a high risk to their users. While there are 15 wallets that hide fake transfers, they are still risky due to displaying zero-value phishing transfers. Only 5 wallets are less risky for displaying only the dust-value phishing transfers. Moreover, only three wallets throw a clear warning message to indicate the risk when users attempt to transfer funds to the phishing address. Therefore, our work implies that it is imperative for the broader crypto wallet developer community to mitigate such a problem. Below, we first discuss what we expect to be achieved in an ideal crypto wallet. Then, we discuss our bug disclosure process and our advice for the crypto wallet users.

5.1 An Ideal Crypto Wallet

Our evaluation shows that no crypto wallets have achieved the highest standard for both usability and security. Here, we discuss what we expect to be achieved by an ideal wallet.

At a high level, an ideal wallet should provide the highest usability and present its users with the lowest risk. Specifically, the ideal wallet should display all legitimate token transfers and transactions, including ETH, USDT, and other legitimate tokens, ensuring that users have access to all legitimate transaction activities. Meanwhile, the wallet should also hide or flag all phishing transfers and transactions to prevent address poisoning attacks from misleading users. To accurately detect the phishing transfers, the wallet can treat fake token transfers, zero-value transfers, and dust-value transfers as suspicious transfers and then match them with a previous legitimate transfer by comparing the address similarity. If the addresses look highly similar, then the suspicious transfers should be flagged. In addition, the ideal wallet should also employ fund recipient verification mechanisms. That is, when the user attempts to transfer assets to a recipient address, the wallet should check whether the address has been flagged by trustworthy sources such as Etherscan and other scam alerting services [8, 14, 21]. If so, the wallet should send an explicit warning message to prompt the user about the potential risk. Moreover, if the recipient address is not flagged by trustworthy sources but is involved in the phishing transfers detected from the user's transaction activity, the wallet should also flag the address as highly risky and alert the user before sending the transaction.

In summary, we believe that the ideal wallet should provide the highest usability and the lowest risk. Meanwhile, the wallet should deploy proactive fund recipient verification mechanisms, which is the last line of defense against the address poisoning attack. By achieving such goals, the wallet can provide users with a high quality service while also safeguarding their crypto assets.

5.2 Bug Report

We have reported the bugs and security risks to the Ethereum crypto wallet developer community. As of this writing, 11 wallets have replied to our bug reports, and 8 have acknowledged our reported problem and are currently deploying countermeasures. While we are awaiting the responses from other crypto wallets, we briefly discuss the mitigation plans of those who confirmed our bug reports. Specifically, Onekey plans to roll out an address book feature and remind users with a highlighted window when the funds are sent to an unknown address. They will also ask users to double-check the transaction details each time. Phantom, which currently displays a warning message when users transfer funds to an unknown address, plans to hide all three types of phishing transfers in the transaction activity feed. Enkrypt confirms that address poisoning is a possible vulnerability, however, they argue that the attack requires human errors and hence do not plan to deploy preventive countermeasures.

5.3 Advice for Wallet Users

While crypto wallets play a crucial role in protecting users' crypto assets, to more effectively mitigate the threat of address poisoning attacks, we also recommend countermeasures for individual wallet users. The most important one is to choose a wallet that provides the strongest security countermeasures, such as phishing transaction detection and labeling, fund recipient address verification, etc. In addition, users should remain vigilant when checking their transaction history and take cautious actions when copying and pasting addresses. It is always a good strategy to verify each character and ensure that the copied address is owned by the correct recipient. Additionally, sending a small test transfer before making a large-value transfer can further confirm that the address is correct and funds will arrive as expected. Another countermeasure that users can adopt is to register an Ethereum Name Record (ENR) for their addresses and use them to send or receive funds, especially when dealing with large-value transfers or sending regular payments to the same recipient. By using the human-readable name instead of the hexadecimal address, users can avoid mistakenly copying phishing addresses that resemble legitimate ones.

6 RELATED WORK

In the existing literature, various cryptocurrency scams and phishing attacks have been studied, including Ponzi [25, 26, 28, 30, 37, 44], fake exchange scams [45], phishings [24, 31, 36], giveaway scams [39, 40, 43, 44], honeypot contract scams [32, 41], scam tokens [34, 46], and token theft [29]. The most relevant work to ours is Guan and Li [35], Tsuchiya et al. [42], and Chen et al. [33], which have studied the three types of phishing transfers utilized in the token-based address poisoning attack. Specifically, Guan and Li [35] developed a detection system and detected over 16 million phishing transfers and 6 million phishing addresses on the Ethereum mainnet. Their work showed that more than 1800 victim transactions lost nearly 100 million US dollars. The similar findings were also reported in Tsuchiya et al. [42]. Chen et al. [33] studied four transaction payload-based phishing scams on Ethereum, including ice phishing, NFT order, address poisoning, and payable function scams. Under the address poisoning category, their work reported that more than 1000 victim transactions lost over 60 million US dollars. Despite the extensive analysis of the address poisoning activities on the Ethereum blockchain, there is a lack of systematic analysis of Ethereum crypto wallets' usability and security under the address poisoning. To our best knowledge, our work is the first one that conducts such a systematic analysis.

7 CONCLUSION

This paper systematically evaluates the usability and security of 53 Ethereum crypto wallets under the address poisoning attack. The evaluation result shows that no wallet achieves the highest usability and security standard, implying further efforts are needed by the broader crypto wallet developer community to address such a problem.

REFERENCES

[1] Binance's loss in the address poisoning attack. https://twitter.com/cz_binance/status/1686764372616515585.

[2] Address poisoning leading to 68 million usd loss. https://x.com/CyversAlerts/status/1786363410243858869, .

[3] Alchemy wallets lists. https://www.alchemy.com/top/wallets, .

[4] Mobile and desktop wallets: What you need to know. https://www.gemini.com/cryptopedia/crypto-wallets-mobile-desktop, .

[5] Binance - cryptocurrency exchange for bitcoin, ethereum. https://www.binance.com/en, .

[6] Bitgo. https://www.bitgo.com/, .

[7] Blockchain explorer. https://www.blockchain.com/explorer/assets/eth, .

[8] Chainabuse. https://www.chainabuse.com/, .

[9] Chainstack: Managed blockchain services. https://chainstack.com/, .

[10] Ethereum tokens. https://cryptoslate.com/blockchain/ethereum/, .

[11] Erc-20 standard. https://en.wikipedia.org/wiki/ERC-20, .

[12] Etherscan: Ethereum (eth) blockchain explorer. https://etherscan.io, .

[13] Getting started: Wallet extension. https://www.coinbase.com/wallet/articles/getting-started-extension, .

[14] Forta. https://www.forta.org/, .

[15] Freewallet. https://freewallet.org/, .

[16] What is a hardware wallet? https://www.coinbase.com/zh-cn/learn/crypto-basics/what-is-a-hardware-wallet, .

[17] Ethereum & ipfs apis. develop now on web 3.0. https://infura.io/, .

[18] Kraken. https://www.kraken.com/, .

[19] Intelligent web3 data platform. https://www.oklink.com/, .

[20] Blockchain infrastructure powering secure, decentralized innovation. https://www.quicknode.com/, .

[21] Scamsniffer. https://www.scamsniffer.io/, .

[22] Whois. https://www.whois.com/, .

[23] Wireshark. https://www.wireshark.org/, .

[24] Emad Badawi, Guy-Vincent Jourdan, Gregor Bochmann, and Iosif-Viorel Onut. An automatic detection and analysis of the bitcoin generator scam. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 407–416. IEEE, 2020.

[25] Massimo Bartoletti, Barbara Pes, and Sergio Serusi. Data mining for detecting bitcoin ponzi schemes. In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pages 75–84. IEEE, 2018.

[26] Massimo Bartoletti, Salvatore Carta, Tiziana Cimoli, and Roberto Saia. Dissecting ponzi schemes on ethereum: identification, analysis, and impact. *Future Generation Computer Systems*, 102:259–277, 2020.

[27] Massimo Bartoletti, Stefano Lande, Andrea Loddo, Livio Pompianu, and Sergio Serusi. Cryptocurrency scams: analysis and perspectives. *Ieee Access*, 9:148353–148373, 2021.

[28] Lingyu Bian, Linlin Zhang, Kai Zhao, Hao Wang, and Shengjia Gong. Image-based scam detection method using an attention capsule network. *IEEE Access*, 9:33654–33665, 2021.

[29] Jiaqi Chen, Yibo Wang, Yuxuan Zhou, Wanning Ding, Yuzhe Tang, XiaoFeng Wang, and Kai Li. Understanding the security risks of decentralized exchanges by uncovering unfair trades in the wild. In *2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P)*, pages 332–351. IEEE, 2023.

[30] Weili Chen, Zibin Zheng, Jiahui Cui, Edith Ngai, Peilin Zheng, and Yuren Zhou. Detecting ponzi schemes on ethereum: Towards healthier blockchain technology. In *Proceedings of the 2018 world wide web conference*, pages 1409–1418, 2018.

[31] Weili Chen, Xiongfeng Guo, Zhiguang Chen, Zibin Zheng, and Yutong Lu. Phishing scam detection on ethereum: Towards financial security for blockchain ecosystem. In *IJCAI*, volume 7, pages 4456–4462, 2020.

[32] Weili Chen, Xiongfeng Guo, Zhiguang Chen, Zibin Zheng, Yutong Lu, and Yin Li. Honeypot contract risk warning on ethereum smart contracts. In *2020 IEEE International Conference on Joint Cloud Computing*, pages 1–8. IEEE, 2020.

[33] Zhuo Chen, Yufeng Hu, Bowen He, Dong Luo, Lei Wu, and Yajin Zhou. Dissecting payload-based transaction phishing on ethereum. In *Network and Distributed Systems Security (NDSS) Symposium*, 2025.

[34] Bingyu Gao, Haoyu Wang, Pengcheng Xia, Siwei Wu, Yajin Zhou, Xiapu Luo, and Gareth Tyson. Tracking counterfeit cryptocurrency end-to-end. *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, 4(3):1–28, 2020.

[35] Shixuan Guan and Kai Li. Characterizing ethereum address poisoning attack, 2024. URL https://doi.org/10.1145/3658644.3690277.

[36] Bowen He, Yuan Chen, Zhuo Chen, Xiaohui Hu, Yufeng Hu, Lei Wu, Rui Chang, Haoyu Wang, and Yajin Zhou. Txphishscope: Towards detecting and understanding transaction-based phishing on ethereum. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, pages 120–134, 2023.

[37] Tyler Kell, Haaroon Yousaf, Sarah Allen, Sarah Meiklejohn, and Ari Juels. Forsage: Anatomy of a smart-contract pyramid scheme. *arXiv preprint arXiv:2105.04380*, 2021.

[38] Kai Li, Shixuan Guan, and Darren Lee. Towards understanding and characterizing the arbitrage bot scam in the wild. *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, 7(3):1–29, 2023.

[39] Kai Li, Darren Lee, and Shixuan Guan. Understanding the cryptocurrency free giveaway scam disseminated on twitter lists. In *2023 IEEE International Conference on Blockchain (Blockchain)*, pages 9–16. IEEE, 2023.

[40] Xigao Li, Anurag Yepuri, and Nick Nikiforakis. Double and nothing: Understanding and detecting cryptocurrency giveaway scams. 2023.

[41] Christof Ferreira Torres, Mathis Steichen, et al. The art of the scam: Demystifying honeypots in ethereum smart contracts. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 1591–1607, 2019.

[42] Taro Tsuchiya, Jin-Dong Dong, Kyle Soska, and Nicolas Christin. Blockchain address poisoning, 2025. URL https://arxiv.org/abs/2501.16681.

[43] Iman Vakilinia. Cryptocurrency giveaway scam with youtube live stream. In *2022 IEEE 13th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, pages 0195–0200. IEEE, 2022.

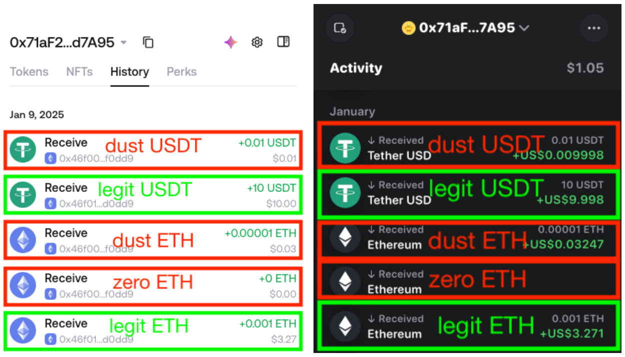
[44] Pengcheng Xia, Haoyu Wang, Xiapu Luo, Lei Wu, Yajin Zhou, Guangdong Bai, Guoai Xu, Gang Huang, and Xuanzhe Liu. Don't fish in troubled waters! characterizing coronavirus-themed cryptocurrency scams. In *2020 APWG Symposium on Electronic Crime Research (eCrime)*, pages 1–14, 2020. doi: 10.1109/eCrime51433.2020.9493255.

[45] Pengcheng Xia, Haoyu Wang, Bowen Zhang, Ru Ji, Bingyu Gao, Lei Wu, Xiapu Luo, and Guoai Xu. Characterizing cryptocurrency exchange scams. *Computers & Security*, 98:101993, 2020.

[46] Pengcheng Xia, Haoyu Wang, Bingyu Gao, Weihang Su, Zhou Yu, Xiapu Luo, Chao Zhang, Xusheng Xiao, and Guoai Xu. Trade or trick? detecting and characterizing scam tokens on uniswap decentralized exchange. *Proc. ACM Meas. Anal. Comput. Syst.*, 5(3), dec 2021. doi: 10.1145/3491051. URL https://doi.org/10.1145/3491051.

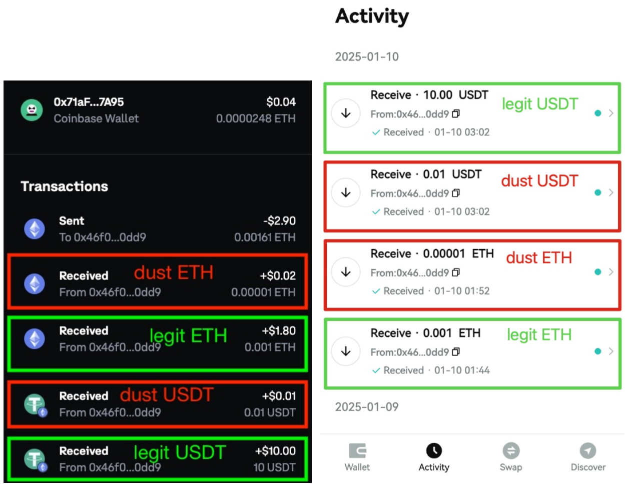
A ETHICAL CONSIDERATION

In this work, we have taken cautious actions to design our experiments. First, our testing transactions are conducted among three Ethereum addresses that are under our control. Although our testing transactions are eventually included


0x71aF2...d7A95
Tokens
NFTs
History
Perks
Jan 9, 2025
Receive dust USDT +0.01 USDT $0.01 0x46f00...f0dd9
Receive legit USDT +10 USDT $10.00 0x46f01...d0dd9
Receive dust ETH +0.00001 ETH $0.03 0x46f00...f0dd9
Receive zero ETH +0 ETH $0.00 0x46f00...f0dd9
Receive legit ETH +0.001 ETH $3.27 0x46f01...d0dd9
0x71aF...7A95
Activity $1.05
January
Received Tether USD dust USDT 0.01 USDT +US$0.009998
Received Tether USD legit USDT 10 USDT +US$9.998
Received Ethereum dust ETH 0.00001 ETH +US$0.03247
Received Ethereum zero ETH
Received Ethereum legit ETH 0.001 ETH +US$3.271

(a) Zerion. (b) Rainbow.

Figure 9: Screenshots of digital wallets at risk level 2.


0x71aF...7A95 $0.04
Coinbase Wallet 0.0000248 ETH
Transactions
Sent -$2.90 To 0x46f0...0dd9 0.00161 ETH
Received dust ETH +$0.02 From 0x46f0...0dd9 0.00001 ETH
Received legit ETH +$1.80 From 0x46f0...0dd9 0.001 ETH
Received dust USDT +$0.01 From 0x46f0...0dd9 0.01 USDT
Received legit USDT +$10.00 From 0x46f0...0dd9 10 USDT
Activity
2025-01-10
Receive · 10.00 USDT legit USDT From:0x46...0dd9 Received · 01-10 03:02
Receive · 0.01 USDT dust USDT From:0x46...0dd9 Received · 01-10 03:02
Receive · 0.00001 ETH dust ETH From:0x46...0dd9 Received · 01-10 01:52
Receive · 0.001 ETH legit ETH From:0x46...0dd9 Received · 01-10 01:44
2025-01-09
Wallet
Activity
Swap
Discover

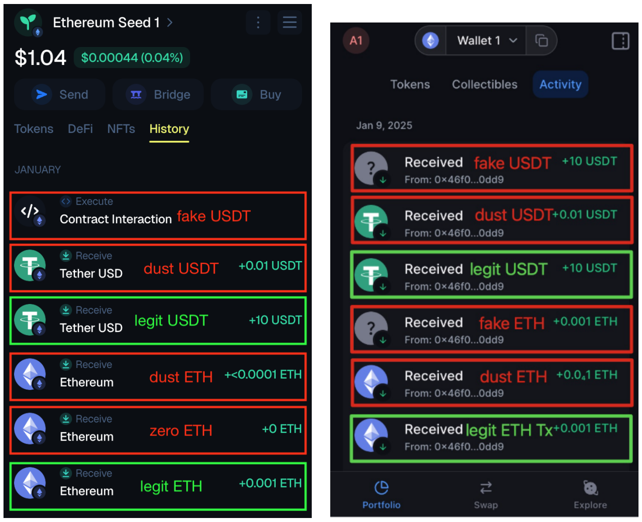
(a) Coinbase. (b) Bitget.

Figure 10: Screenshots of digital wallets at risk level 1.

in the Ethereum mainnet, they do not affect other addresses or users on Ethereum. Besides, our analysis of 53 Ethereum crypto wallets is also conducted on our own laptop, which is a controlled environment and does not affect other wallet users. Moreover, throughout the paper, we have tried our best to anonymize phishing addresses controlled by others through shortening their addresses. Finally, we have reported the usability bugs and security risks to the crypto wallet developer community and recommended mitigation solutions against the address poisoning threat. We hope to help them achieve the highest usability and security standard.

B MORE SCREENSHOTS OF ETHEREUM WALLETS

This section presents the screenshots of displayed transfers on other crypto wallets. Fig. 8 shows the transfers displayed on wallet Nest and Backpack, which were assigned at risk level 3. Fig. 9 shows the transfers displayed on wallet Zerion and Rainbow, which were assigned at risk level 2. Fig. 10 shows the transfers displayed on wallets Coinbase and Bitget, which were assigned at risk level 1.


Ethereum Seed 1
$1.04 $0.00044 (0.04%)
Send
Bridge
Buy
Tokens
DeFi
NFTs
History
JANUARY
Execute Contract Interaction fake USDT
Receive Tether USD dust USDT +0.01 USDT
Receive Tether USD legit USDT +10 USDT
Receive Ethereum dust ETH +<0.0001 ETH
Receive Ethereum zero ETH +0 ETH
Receive Ethereum legit ETH +0.001 ETH
A1
Wallet 1
Tokens
Collectibles
Activity
Jan 9, 2025
Received fake USDT +10 USDT From: 0×46f0...0dd9
Received dust USDT +0.01 USDT From: 0×46f0...0dd9
Received legit USDT +10 USDT From: 0×46f0...0dd9
Received fake ETH +0.001 ETH From: 0×46f0...0dd9
Received dust ETH +0.0,1 ETH From: 0×46f0...0dd9
Received legit ETH Tx +0.001 ETH From: 0×46f0...0dd9
Portfolio
Swap
Explore

(a) Nest. (b) Backpack.

Figure 8: Screenshots of digital wallets at risk level 3.