ABSTRACT

With the growth of the cryptocurrency ecosystem, there is expanding evidence that counterfeit cryptocurrency has also appeared. In this paper, we empirically explore the presence of counterfeit cryptocurrencies on Ethereum and measure their impact. By analyzing over 190K ERC-20 tokens (or cryptocurrencies) on Ethereum, we have identified 2,117 counterfeit tokens that target 94 of the 100 most popular cryptocurrencies. We perform an end-to-end characterization of the counterfeit token ecosystem, including their popularity, creators and holders, fraudulent behaviors and advertising channels. Through this, we have identified two types of scams related to counterfeit tokens and devised techniques to identify such scams. We observe that over 7,104 victims were deceived in these scams, and the overall financial loss sums to a minimum of $17 million (74,271.7 ETH). Our findings demonstrate the urgency to identify counterfeit cryptocurrencies and mitigate this threat.

1 INTRODUCTION

Since the first Bitcoin block was mined in 2009, cryptocurrencies have seen significant growth. This growth is mainly due to the rapid development of blockchain technologies and the digital economic system. Where there is money, there are those who follow it. Cryptocurrencies have attracted extensive attention from attackers. Attackers have exploited the vulnerabilities in smart contracts, cryptocurrency exchanges and wallets. However, an understudied attack is counterfeit money — the imitation of currency, which is produced without the legal sanction of the government. Fraudsters strive to imitate the official currency so as to deceive its recipient. Following the same postulation, we ask if such kinds of counterfeit money have appeared in the cryptocurrency ecosystem?

Moreover, the ease of creating cryptocurrencies and launching Initial Coin Offerings (ICO), makes the cost of releasing counterfeit cryptocurrencies quite low. For example, Ethereum, as an open-source platform for decentralized applications (DApps), is the first blockchain platform that simplifies the development of smart contracts. Based on Ethereum, one can create a token smart contract with just a few lines of code. By July 2020, there were over 200 thousand ERC-20 tokens created on Ethereum. However, Ethereum does not enforce any restrictions on the names and symbols of the newly created tokens. Instead, the thing that identifies a token is its smart contract address. This opens up a number of potential fraudulent avenues, with malicious parties potentially exploiting this fact to counterfeit cryptocurrencies.

Despite this, to the best of our knowledge, the counterfeit cryptocurrency ecosystem has not been systematically investigated or measured. Thus, there is a general lack of an understanding of this attack, including: 1) to what extent counterfeit cryptocurrencies exist; 2) what are the entities related to the counterfeit cryptocurrencies, i.e., their targets, creators, distributors, and users; 3) what are they used for, i.e., whether counterfeit cryptocurrencies are involved in blockchain scams; and 4) the advertising channels of counterfeit cryptocurrencies, i.e., how do they reach and attract victims.

In this paper, we present the first systematic study of counterfeit cryptocurrencies on Ethereum. By analyzing over 170K ERC-20 tokens created on Ethereum, we have identified 2,117 counterfeit tokens that target 94 of the top-100 most popular cryptocurrencies (tokens). We then analyze the distribution and popularity of these counterfeit tokens, as well as the creators and holders of them. After identifying two types of fraudulent behaviors related to the counterfeit cryptocurrencies, we further measure the impacts of the counterfeit cryptocurrency ecosystem, including the scale of the financial losses and the number of victims. Finally, to further understand how they are spread, we go a further step to investigate the advertising channels of these counterfeit cryptocurrencies.
### Table 1: Summary of the scams we identified.

| Type            | # Transactions | Scam Address                  | # Victims | # ETH        | # USD       |
|-----------------|----------------|-------------------------------|-----------|-------------|-------------|
| Airdrop Scam    | 2,872          | Counterfeit Token Address     | 87        | 2,037       | 970.8       | 226,817.71  |
|                 |                | Counterfeit Token Creator     | 71        |             |             |             |
|                 |                | ETH Received Address          | 70        |             |             |             |
|                 |                | Counterfeit Token Distributed Address | 56 |     |             |             |
|                 |                | Sum                           | 166       |             |             |             |
| Arbitrage Scam  | 7,617          | Counterfeit Token Address     | 486       | 5,087       | 73,300.9    | 17,126,022.30 |
|                 |                | Counterfeit Token Creator     | 293       |             |             |             |
|                 |                | ETH Received Address          | 1,879     |             |             |             |
|                 |                | Counterfeit Token Distributed Address | 869 |     |             |             |
|                 |                | Sum                           | 2,904     |             |             |             |
| Sum             | 10,489         | 3,053 (565 counterfeit tokens involved) | 7,104 | 74,271.7 | 17,352,840.00 |

### 2 MAIN RESULTS

#### 2.1 Are counterfeit cryptocurrencies prevalent in the cryptocurrency ecosystem?

Counterfeit tokens are indeed prevalent in the cryptocurrency ecosystem. We have identified 2,117 counterfeit tokens targeting 94 out of the 100 tokens we studied. Although most of the tokens have very few transactions, some of them are quite popular, with thousands of transactions and holders. Malicious actors tend to target more than one type of official token, mainly due to the cost of creating a counterfeit token is quite low in Ethereum.

#### 2.2 What are the fraudulent behaviors related to counterfeit cryptocurrencies?

We have identified two types of scams related to counterfeit tokens, i.e., airdrop scam and the arbitrage scam.

##### 2.2.1 Airdrop Scam

Airdrops are primarily implemented as a way of gaining attention and new followers. As airdrops are quite popular for well-known tokens, counterfeit tokens are also taking advantage of this opportunity to perform airdrop scams. In general, the attackers promise that, after sending a certain amount of ETH to the (counterfeit) token address, the victim will get (imitated) official tokens according to a fixed exchange rate (far more than the actual value). After victims send the ETH, they likely only receive counterfeit tokens of no value at all.

##### 2.2.2 Arbitrage Scam

Arbitrage is an investment method that capitalizes on imbalances in prices between markets, i.e., buy at a low price and sell at a slightly higher price. From the perspective of amateur investors, the arbitrage does not require too much professional knowledge, which is relatively safer compared with other investment methods. Thus, cryptocurrency arbitrage is popular among many investors. However, our exploration suggests that the arbitrage can be abused by attackers, i.e., the arbitrage can be combined with counterfeit tokens to carry out well-designed scams. In our collected scams, the scammers usually use fake Telegram groups (that imitate the official token) as advertising channels, providing scam addresses for victims to send ETH. After victims send ETH to the specified scam address, as promised, they should get official tokens (far more than the actual value) in a few minutes. However, victims usually received counterfeit tokens of no worth.

##### 2.2.3 Overall Results

Table 1 shows the overall results. In total, 565 active counterfeit tokens have been found involved with scams. Over 7,100 victims were deceived, and the overall financial loss sums to a minimum amount of $17 million (74,271.7 ETH).

### Table 2: A Summary of the advertising channels.

| Channel Type | Arbitrage | Airdrop | Sum |
|--------------|-----------|---------|-----|
| Telegraph Page | 589       | 4       | 593 |
| Telegram Group | 52        | 76      | 128 |
| Twitter Page | 0         | 25      | 25  |
| Facebook Page | 0         | 22      | 22  |
| YouTube | 0         | 5       | 5   |
| Others | 20        | 142     | 162 |
| Sum of Pages | 661       | 274     | 935 |
| Channel Type | 11        | 96      | 103 |

#### 2.3 What are the advertisement channels of counterfeit cryptocurrencies?

As shown in Table 2, a number of reputable platforms have been abused by attackers to help spread fraudulent information on counterfeit tokens. Social network platforms like Telegram, Twitter and Facebook are the main targets of attackers. Various social engineering techniques have been adopted to trick users.

### ACKNOWLEDGMENT

The full paper appears at [1]. This work was supported by the National Natural Science Foundation of China (grants No.61702045 and No.62072046), Hong Kong RGC Project (No. 152193/19E), the Fundamental Research Funds for the Central Universities, Leading Innovative and Entrepreneur Team Introduction Program of Zhejiang (2018R01005). Haoyu Wang (haoyuwang@bupt.edu.cn) is the corresponding author.

### REFERENCES

[1] Bingyu Gao, Haoyu Wang, Pengcheng Xia, Siwei Wu, Yajin Zhou, Xiapu Luo, and Gareth Tyson. 2021. Tracking Counterfeit Cryptocurrency End-to-end. Proc. ACM Meas. Anal.Comput. Syst. 4, 3 (2021).