Poster: An Empirical Study of Backdoor Attacks on Ethereum Smart Contracts

Naoto Yanai
Panasonic Holdings Corportation
yanai.naoto@jp.panasonic.com

Naohisa Nishida
Panasonic Holdings Corportation
nishida.naohisa@jp.panasonic.com

Yuji Unagami
Panasonic Holdings Corportation
unagami.yuji@jp.panasonic.com

Abstract—**Backdoor attacks on Ethereum smart contracts are attacks where an adversary exploits the privileges of his/her developed smart contracts to manipulate assets generated by the contracts. In this paper, we conduct an empirical study to identify how many backdoor attacks are performed in the real world. As a result, we totally found 288440 backdoors. The most major backdoor attack is ArbitraryTransfer, which transfers assets into any address, and there are 189874 smart contracts for this attack. Another insight is that several backdoor attacks are combined with other backdoors. Remarkably, more than 90% of DisableTransfer, which disables transfers of assets into other addresses, are combinations with other backdoor attacks.**

I. Introduction

Ethereum smart contracts [1] have been widely utilized as a tool to develop distributed applications and tokens for cryptoassets. Ethereum smart contracts are programs deployed on peer-to-peer (P2P) networks for blockchains and enable users to execute the programs themselves by sending Ether as cryptocurrency. (Hereafter, we refer to Ethereum smart contracts simply as ”smart contracts.”)

Backdoor attacks (also known as rug pull) are security issues on smart contracts [2]. Loosely speaking, an adversary with backdoor attacks develops smart contracts and then maliciously utilizes their privilege to manipulate cryptoassets such as cryptocurrency or tokens. At Australia in June 2018, 6.6M$ were stolen from Soarcoin by backdoor attacks[1]. Nevertheless, to the best of our knowledge, the existing empirical studies about the backdoor attacks are limited. An empirical study for backdoor attacks is crucial since it can shed light on the financial impact, as well as the direction of subsequent works.

In this paper, we investigate *how many backdoor attacks occur* and *what the most frequent methods are for backdoor attacks* as an empirical study for backdoor attacks on smart contracts. To this end, we analyzed 66,283,849 smart contracts with source codes, which were generated by May 2024, with several backdoor detection tools [3], [4].

II. Technical Background

1) Smart Contracts and Their Backdoors Attacks: Smart contracts are implemented by a high-level language such as Solidity, and there are eight major compiler versions from v0.1 to v0.8 for Solidity. Once deployed on blockchains, smart contracts are operated by peers with Ethereum virtual machines (EVMs) on P2P networks. Each smart contract is assigned a contract address and then can receive Ether and execute its functions through the contract address. Peers can obtain Ether as gas when their EVMs execute smart contracts. Recent smart contracts can also provide various applications, not only cryptocurrency but also tokens as cryptoassets [5].

For backdoor attacks on smart contracts below, users with cryptoassets created from smart contracts for backdoor attacks (named contract backdoors for the sake of convenience) may lose their cryptoassets or accounts [3]. Specifically, we say that smart contracts are contract backdoors if (1) they contain executable functions for only a user with privilege, e.g., a developer of smart contracts, and (2) they affect cryptoassets of other users. There are five methods [3], i.e., ArbitrarilyTransfer to transfer cryptoassets into any address, GenerateTokens to mint new tokens, DestroyTokens to destroy cryptoassets on any contract address, DisableTransfer to disable transferring into certain accounts, and FreezeAccount to freeze certain accounts directly by the owner. We investigate these methods although we omit their details due to the space limitation.

2) Related Works: As empirical results in the existing works [5], [6], the lifetime of more than 60% of contract backdoors is shorter than one day [5] and 7487 contract backdoors for non-fungible tokens have been found [6]. We investigate contract backdoors for all the deployed smart contracts with source code.

III. Problem Setting

In this paper, we collected all the smart contracts deployed on the Ethereum blockchain from 2015/08/07 to 2024/05/31 and then analyzed their source code. Specifically, we focus on static analysis of Solidity and hence utilize Etherscan[2], a publicly available explorer for the Ethereum blockchain, to collect the smart contracts whose source code is available. We then collected 66,283,849 smart contracts. When we removed smart contracts whose bytecode is duplicated or `0x`,

[1] nz.finance.yahoo.com/news/backdoor-flaw-sees-australian-firm-115323212.html

[2] https://etherscan.io/

Network and Distributed System Security (NDSS) Symposium 2025
24-28 February 2025, San Diego, CA, USA
ISBN 979-8-9894372-8-3
https://dx.doi.org/10.14722/ndss.2025.[23|24]xxxx
www.ndss-symposium.org

TABLE I
Number of Contract Backdoors for Each Compiler Version

Values for each attack represent the number of contract backdoors, and ones with parentheses represent the ratio with the column of "Number of Contracts". The column of "Number of Backdoors" represents the number of smart contracts that are detected as at least one of the five methods, which is different from the summation of values for the five methods.

	Number of Contracts	ArbitraryTransfer	GenerateToken	DestroyToken	DisableTransfer	FrozenAccount	Number of Backdoors
v0.1	28	4 (14.3%)	1 (3.6%)	0 (0%)	3 (10.7%)	0 (0%)	4 (14.3%)
v0.2	88	5 (5.7%)	4 (4.5%)	0 (0%)	5 (5.7%)	0 (0%)	9 (10.2%)
v0.3	556	78 (14.0%)	43 (7.9%)	0 (0%)	70 (12.6%)	0 (0%)	106 (19.1%)
v0.4	82567	24706 (29.9%)	21405 (25.9%)	717 (0.9%)	18789 (22.8%)	2560 (3.1%)	34863 (42.2%)
v0.5	46334	8679 (18.7%)	13663 (29.5%)	39 (0.1%)	7708 (16.6%)	333 (0.7%)	10248 (22.2%)
v0.6	50005	6573 (13.1%)	15012 (30%)	30 (0.1%)	8798 (17.6%)	194 (0.4%)	18027 (36.1%)
v0.7	37163	2536 (6.8%)	4951 (13.3%)	15 (0%)	3018 (8.1%)	118 (0.3%)	6786 (18.3%)
v0.8	466414	147293 (31.6%)	87118 (18.7%)	1997 (0.4%)	173296 (37.2%)	44704 (9.6%)	218397 (46.8%)
Total	683153	189874 (27.8%)	142197 (20.5%)	2798 (0.4%)	211687 (31.0%)	47909 (7.01%)	288440 (42.2%)

we obtained 1,271,127 smart contracts in total. The static analysis is executed with the existing tools [3], [4] to identify backdoors. In doing so, we define that a smart contract is a contract backdoor as long as either of the existing tools detects it as a backdoor. The smart contracts are analyzed for each compiler version since the specification of the compiler may affect backdoor attacks.

IV. Result and Discussion

We show the results in Table I and discuss their insights below. The first insight is that 42.2% of the smart contracts are contract backdoors. The version with the largest number of contract backdoors is v0.8, and 46.8% of the smart contracts for this version are the backdoors. When we manually identify these smart contracts, they also contain potential contract backdoors that have only a portion of the functions for the backdoors. In other words, they may become contract backdoors by additionally developing several functions for the backdoors. The largest backdoor contracts are DisableTransfer, and 31.0% of the smart contracts are this backdoor.

When we analyzed these contract backdoors, we found the second insight. According to Fig. 1, many contract backdoors are based on combinations with other kinds of the backdoors. Remarkably, whereas there are 173296 contract backdoors for DisableTransfer in v0.8, 15195 contracts contain only DisableTransfer. In other words, more than 90% of the contract backdoors for DisableTransfer are combinations with the others. It means that DisableTransfer is often combined as a building block of the other backdoors. Further investigation into these combinations needs to be undertaken.

Finally, we briefly describe threats to validity in this paper. There were 169000 smart contracts that the tools returned errors during the analysis. They may contain further contract backdoors. Our results also depend on the utilized tools.

V. Conclusion

In this paper, we conducted an empirical study to identify how many backdoor attacks are performed in the real world. When we analyzed all the smart contracts deployed from 2015/08/07 to 2024/05/31, we found 288440 contract backdoors. The most major backdoor attack was ArbitraryTransfer, and we found 189874 contract backdoors for this attack. We also demonstrated that more than 90% of DisableTransfer are combinations with the other backdoor attacks. We plan to investigate each contract backdoor, including the above combinations, in detail.

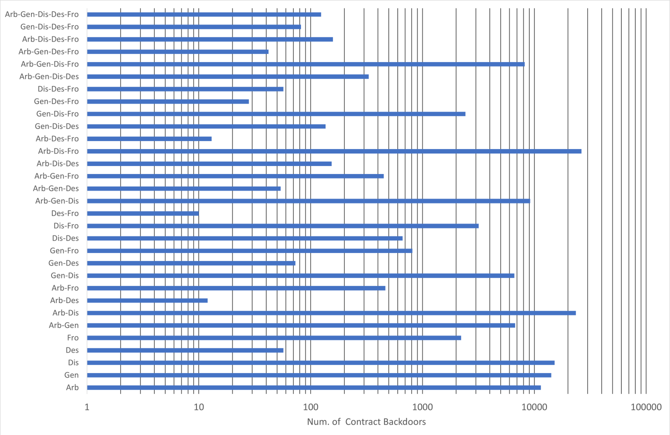


Fig. 1. The number of contract backdoors for each combination in v0.8.

References

[1] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger byzantium version," https://ethereum.github.io/yellowpaper/paper.pdf, 2022.

[2] D. Sun, W. Ma, L. Nie, and Y. Liu, "Sok: Comprehensive analysis of rug pull causes, datasets, and detection tools in defi," *CoRR*, vol. abs/2403.16082, 2024. [Online]. Available: https://doi.org/10.48550/arXiv.2403.16082

[3] F. Ma, M. Ren, L. Ouyang, Y. Chen, J. Zhu, T. Chen, Y. Zheng, X. Dai, Y. Jiang, and J. Sun, "Pied-piper: Revealing the backdoor threats in ethereum erc token contracts," *ACM Transactions on Software Engineering and Methodology*, vol. 32, no. 3, pp. 1–24, 2023.

[4] Z. Lin, J. Chen, J. Wu, W. Zhang, Y. Wang, and Z. Zheng, "Crpwarner: Warning the risk of contract-related rug pull in defi smart contracts," *IEEE Transactions on Software Engineering*, vol. 50, no. 6, pp. 1534–1547, 2024.

[5] F. Cernera, M. La Morgia, A. Mei, and F. Sassi, "Token spammers, rug pulls, and sniper bots: An analysis of the ecosystem of tokens in ethereum and in the binance smart chain ({{{{{BNB}}}}})," in *PRoc. of USENIX Security 2023*. Usenix Security, 2023, pp. 3349–3366.

[6] J. Huang, N. He, K. Ma, J. Xiao, and H. Wang, "A deep dive into NFT rug pulls," *CoRR*, vol. abs/2305.06108, 2023. [Online]. Available: https://doi.org/10.48550/arXiv.2305.06108

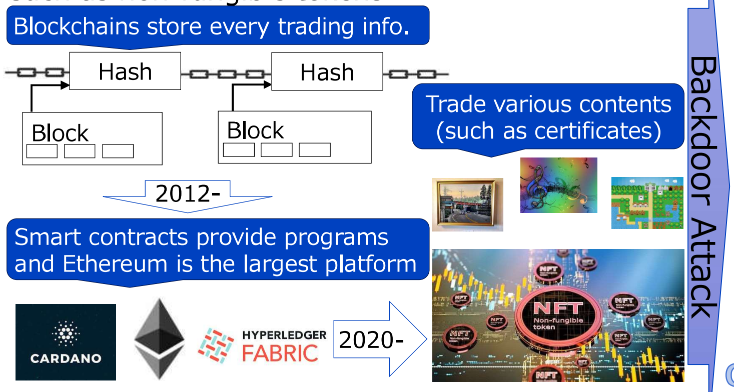
An Empirical Study of Backdoor Attacks on Ethereum Smart Contracts

(This research is supported by JST SAKIGAKE, JPMJPR23P6.)

Naoto Yanai, Naohisa Nishida, Yuji Unagami (Panasonic Holdings Corp.)

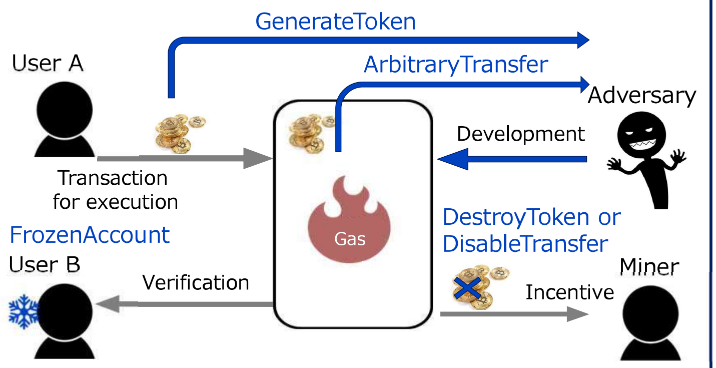
Ethereum Smart Contracts and Their Backdoor Attacks

Blockchains are from currency to creation of assets, such as non-fungible tokens


Blockchains store every trading info.
Hash
Hash
Block
Block
Trade various contents (such as certificates)
2012-
Smart contracts provide programs and Ethereum is the largest platform
CARDANO
HYPERLEDGER FABRIC
2020-
NFT
Non-fungible token
Backdoor Attack

As the dark side, there are several malicious use

Develop malicious contracts to affect assets [1]



Q1: How many backdoor attacks take place?

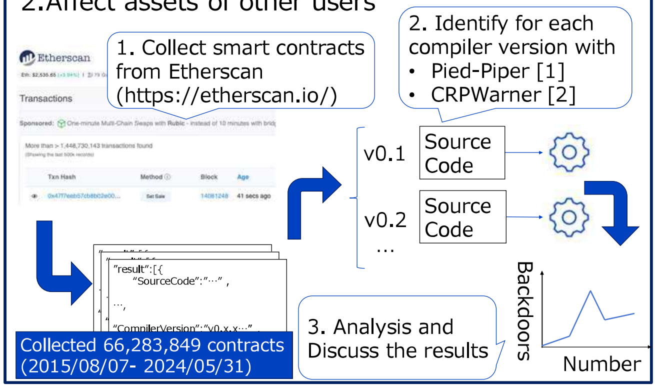
Q2: What methods are used in these attacks?

Study Overview

Smart contracts are contract backdoors if

1.Contain functions executed by privileged users

2.Affect assets of other users


1. Collect smart contracts from Etherscan (https://etherscan.io/)
2. Identify for each compiler version with
• Pied-Piper [1]
• CRPWarner [2]
Etherscan
Transactions
Txn Hash
Method
Block
Age
"result":[{
"SourceCode":"…" ,
…,
"CompilerVersion":"v0.x.x…" ,
v0.1
Source Code
v0.2
Source Code
…
3. Analysis and Discuss the results
Backdoors
Number

Collected 66,283,849 contracts (2015/08/07- 2024/05/31)

Main Result

42.2% of smart contracts are backdoors

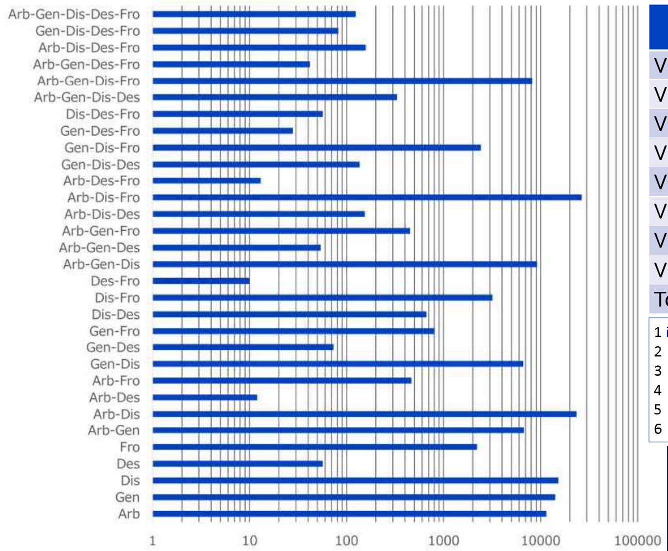
- v0.8 contains the largest number of contract backdoors
- DisableTransfer is the largest among the current backdoors

	Num. of Contracts	Arbitrary Transfer	Generate Token	Destroy Tokens	Disable Transfer	Frozen Account	Num. of Backdoors
V0.1	28	4	1	0	3	0	4
V0.2	88	5	4	0	5	0	9
V0.3	556	78	44	0	70	0	106
V0.4	82567	24706	21405	717	18789	2560	36863
V0.5	46334	8679	13663	39	7708	333	10248
V0.6	50005	6573	15012	30	8798	194	18027
V0.7	37163	2536	4951	15	3018	118	6786
V0.8	466414	147293	87118	1997	173296	44704	218397
Total	683153	189874	142198	2798	211687	47909	288440

Discussion

Many backdoors are combinations with others

- More than 90% of DisableTransfer are combinations
- ArbitraryTransfer and DisableTransfer are a major pairs
  →Stop the transfer and then change its destination



For the number of backdoors without combinations

- GenerateToken and DisableTokens are limited (>10%)
- They just disturb transactions and give no financial advantages to an adversary

	Num. of Backdoors	Arbitrary Transfer	Generate Token	Destroy Tokens	Disable Transfer	Frozen Account	Total w/o Comb.
V0.1	4	0	0	0	0	0	0
V0.2	9	2	2	0	1	0	5
V0.3	106	8	11	0	14	0	33
V0.4	36863	6497	4811	81	1764	354	13507
V0.5	10248	3070	6186	3	1087	77	10423
V0.6	18027	775	6817	2	766	114	8474
V0.7	6786	383	1766	2	455	46	2652
V0.8	218397	11460	14184	57	15195	2215	43111
Total	288440	22195	33777	145	19282	2806	78205

```
if ( msg . sender == contractPreICO || msg . sender == contractICO ){  // DisableTransfer (to restrict allowable users)
   if( partnersPromo [ promo ] != address (0 x0) && partnersPromo [ promo ] != referral ){
         partner = partnersPromo [ promo];
         referrals [ referral ] += amount ;  // GenerateToken (to increase assets of the adversary)
         amount_referral_invest += amount ;
         partnersInfo [ partner ]. Balance += amount ;
```

Ethical consideration: We cause neither financial incentives for an adversary nor new victims through our study because

- We only collected smart contracts and did not develop new one
- We executed static analysis and did not run these smart contracts

[1] F. Ma et al., "Pied-Piper: Revealing the backdoorthreats in Ethereum ERC token contracts," ACM Transactions on Software Engineering and Methodology, vol. 32, no. 3, pp. 1–24, 2023.
[2] Z. Lin et al., "CRPWarner:Warning the risk of contract-related rug pull in defi smart contracts," IEEE Transactions on Software Engineering, vol. 50, no. 6, pp. 1534–1547, 2024.