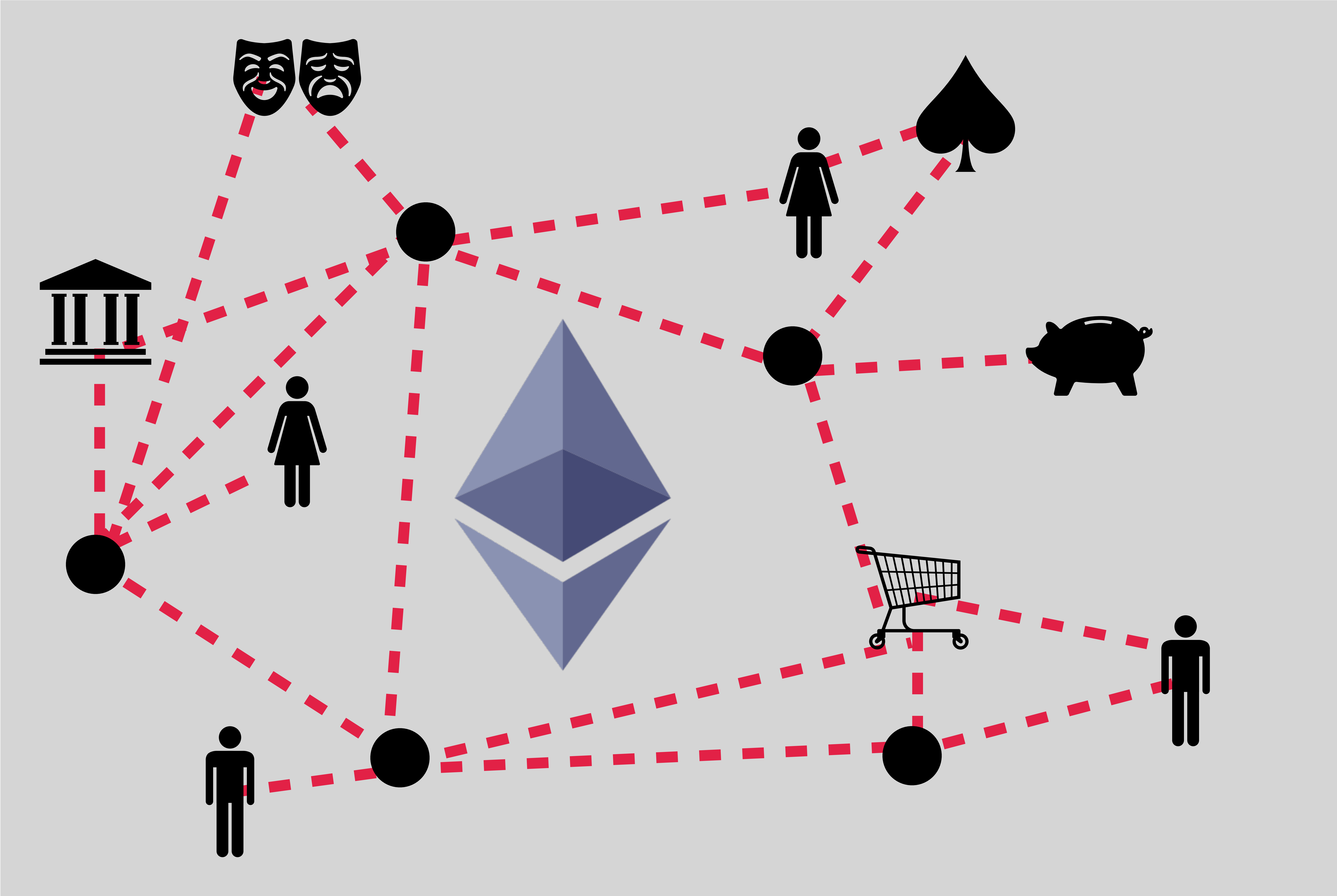
Evil Under the Sun: Understanding and Discovering Attacks on Ethereum Decentralized Applications

Liya Su[1,2,3] Xinyue Shen[1,4] Xiangyu Du[1,2,3] Xiaojing Liao[1]
XiaoFeng Wang[1] Luyi Xing[1] Baoxu Liu[2]

[1]Indiana University Bloomington
[2]Institute of Information Engineering, Chinese Academy of Sciences,
[3]University of Chinese Academy of Sciences
[4]Alibaba Group

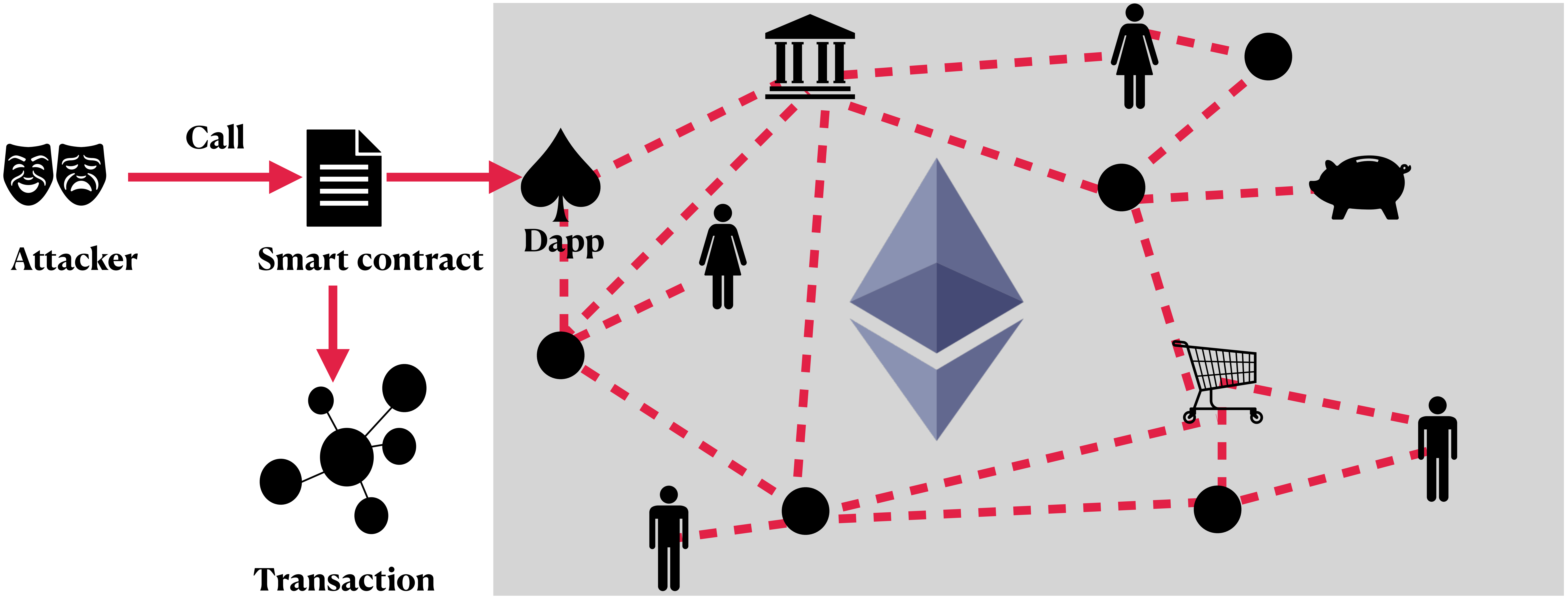
Background



- Ethereum: computer programs on the blockchain
- Externally Owned Accounts (EOAs)
- Smart Contract: deploy on Ethereum
- Dapp: public smart contract

Background

Dapp Attack



Background

3,137 Dapps

63.77k active users

Over 1 million transactions

7.55 million USD

Requirement

Facts

14K Ethers from the victim Fomo3D

No extensive forensic analysis

Research Questions

What like and how the attacks launch on real-world Dapps?

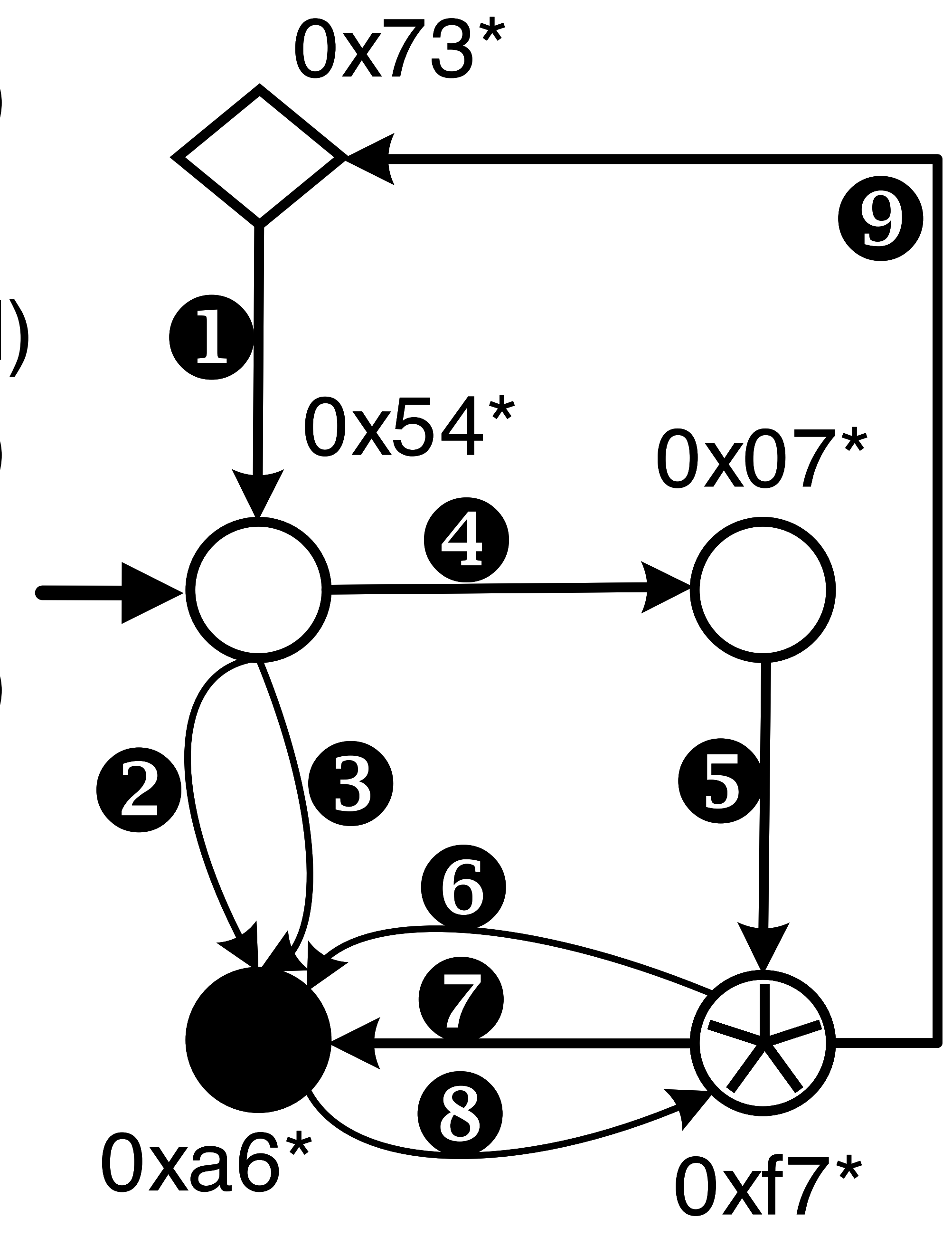
How to automatically reconstruct Dapp attacks?

How to find new attack and 0-day victim Dapps?

Transaction based Forensic Analysis

TO	0x54*
FROM	0x73*
VALUE	0.01 Ether
DATA	0xc52ab778 (methodID of function execute())
GAS PRICE	$6.3x10^{-9}$ Ether (6.3 Gwei)

❶ (0x73*, 0x54*, execute(0xa6*), 0.1 ETH)
❷ (0x54*, 0xa6*, airDropPot_(), 0 ETH)
❸ (0x54*, 0xa6*, airDropTracker_(), 0 ETH)
❹ (0x54*, 0x07*, execute(0xa6*), 0.1 ETH)
❺ (0x07*, 0xf7*, create, 0.1 ETH)
❻ (0xf7*, 0xa6*, buyXid(0x0000), 0.1 ETH)
....
❼ (0xf7*, 0xa6*, withdraw(), 0 ETH)
❽ (0xa6*, 0xf7*, transfer, 0.1012 ETH)
❾ (0xf7*, 0x73*, suicide, 0.1012 ETH)



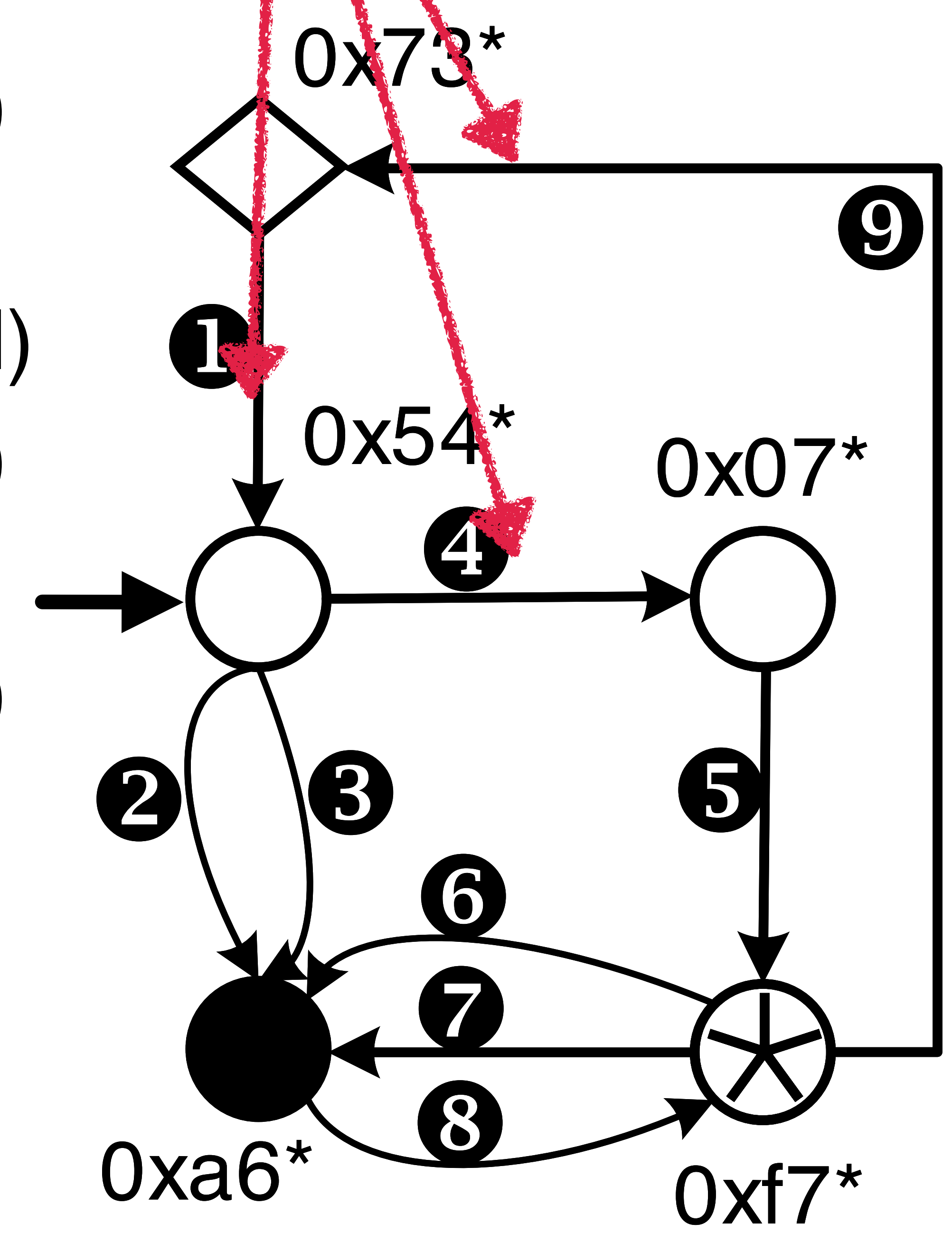
Background

A Transaction data package

TO	0x54*
FROM	0x73*
VALUE	0.01 Ether
DATA	0xc52ab778 (methodID of function execute())
GAS PRICE	6.3x10^{-9} Ether (6.3 Gwei)

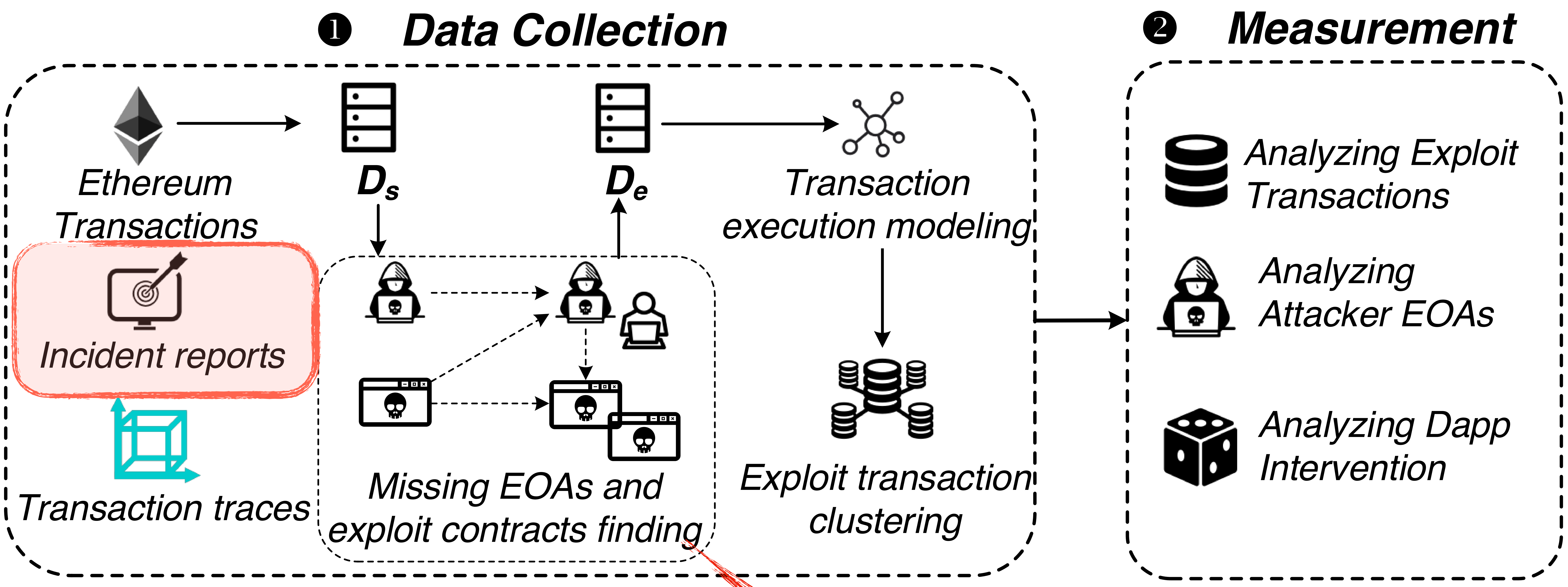
Transaction's Execution Trace

❶ (0x73*, 0x54*, execute(0xa6*), 0.1 ETH)
❷ (0x54*, 0xa6*, airDropPot_(), 0 ETH)
❸ (0x54*, 0xa6*, airDropTracker_(), 0 ETH)
❹ (0x54*, 0x07*, execute(0xa6*), 0.1 ETH)
❺ (0x07*, 0xf7*, create, 0.1 ETH)
❻ (0xf7*, 0xa6*, buyXid(0x0000), 0.1 ETH)
....
❼ (0xf7*, 0xa6*, withdraw(), 0 ETH)
❽ (0xa6*, 0xf7*, transfer, 0.1012 ETH)
❾ (0xf7*, 0x73*, suicide, 0.1012 ETH)



Example of transaction execution traces.
○ : exploit contract, ⊗: contract generated in execution, ●: Dapp, ◇: EOA.

Analyzing Exploit Transactions



Workflow of the measurement approach.

Data Collection and Derivation

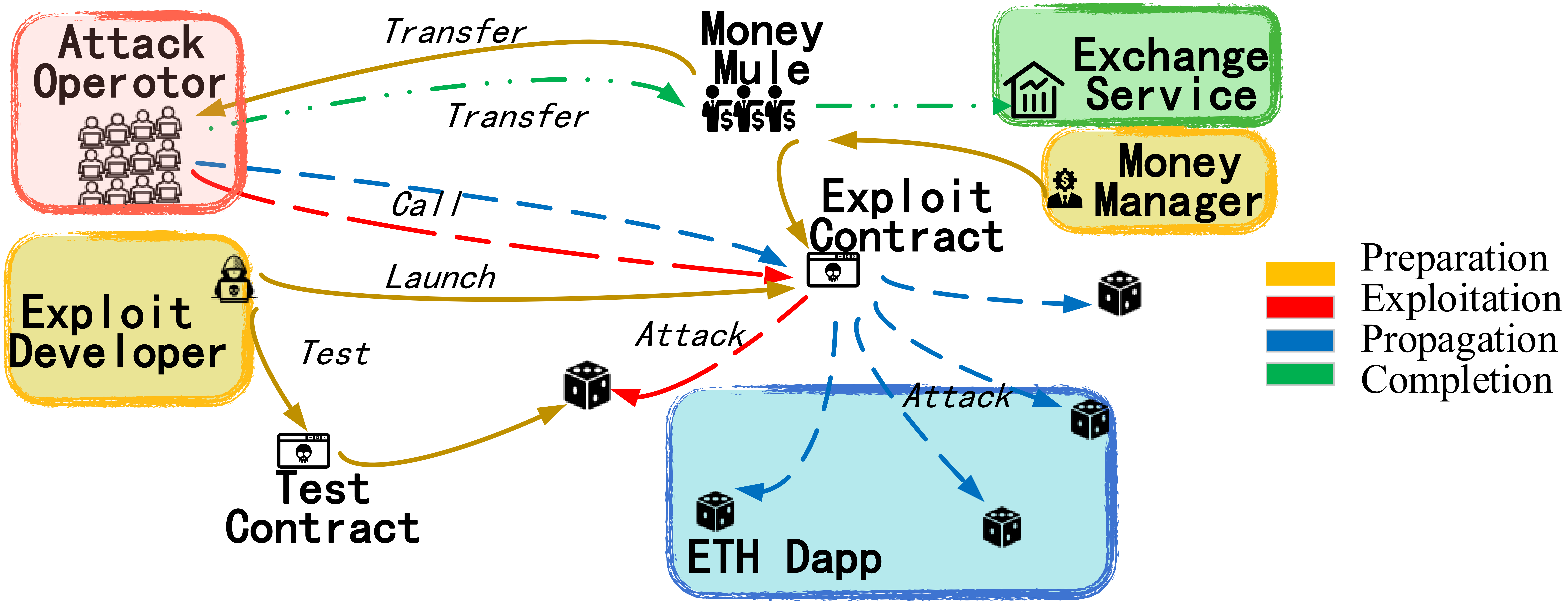
Analyzing Exploit Transactions

Data Collection and Derivation

Table 2: Known Dapp attacks. D_s is the set of data collected from the reports, and D_e includes those derived.

Attack type	# of Dapps		# of exploit contracts		# of attacker EOAs		# of attack transactions	
	D_s	D_e	D_s	D_e	D_s	D_e	D_s	D_e
Bad randomness	4	14	9	19	9	27	14	40,766
DoS	4	6	3	3	5	88	4	17,088
Integer overflow/underflow	13	32	1	2	28	53	47	591
Reentrancy	2	2	2	3	2	4	2	30
Improper authentication	12	18	6	18	17	60	34	575
Unique total	25	56	20	45	48	227	77	58,555

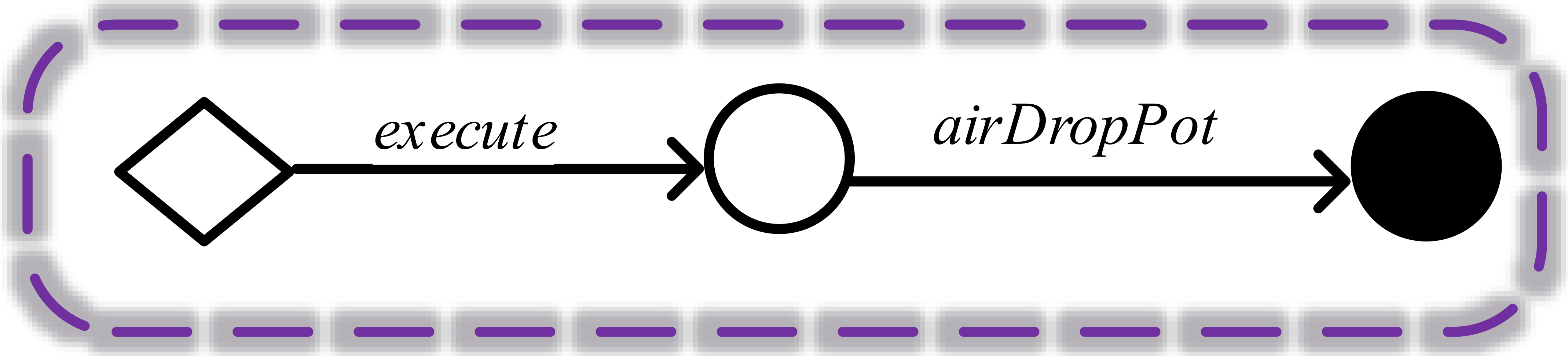
Analyzing Exploit Transactions

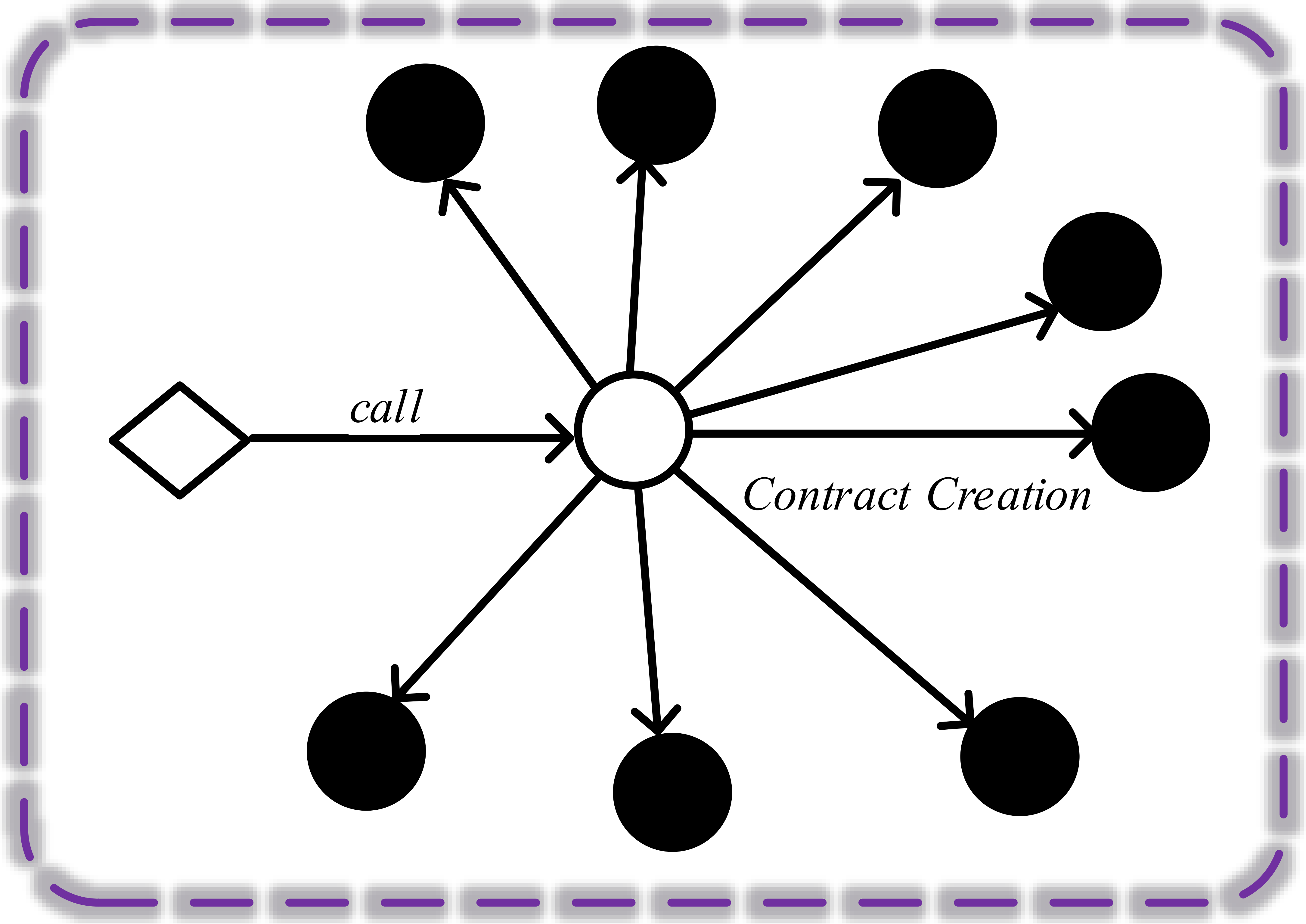


Example of Dapp criminal footprints.

Analyzing Exploit Transactions

Preparation: Testing contracts or transferring fund

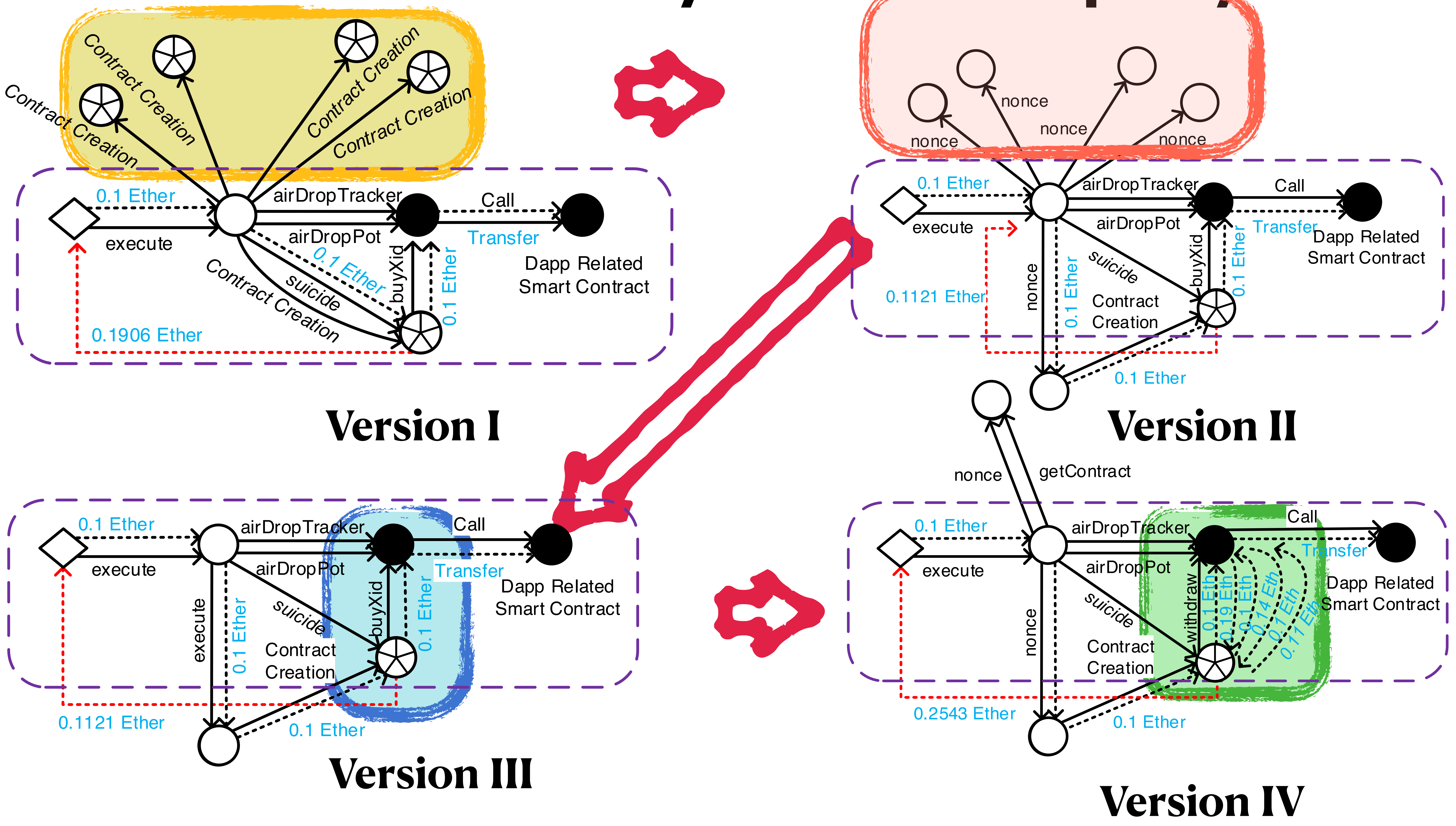




Testing transaction in preparation stage.

Analyzing Exploit Transactions

Exploitation: The adversary tends to rapidly evolve his strategies



Exploit contract evolution at the exploitation stage.

average TG distance = 0.4

DEFIER: Idea and Design

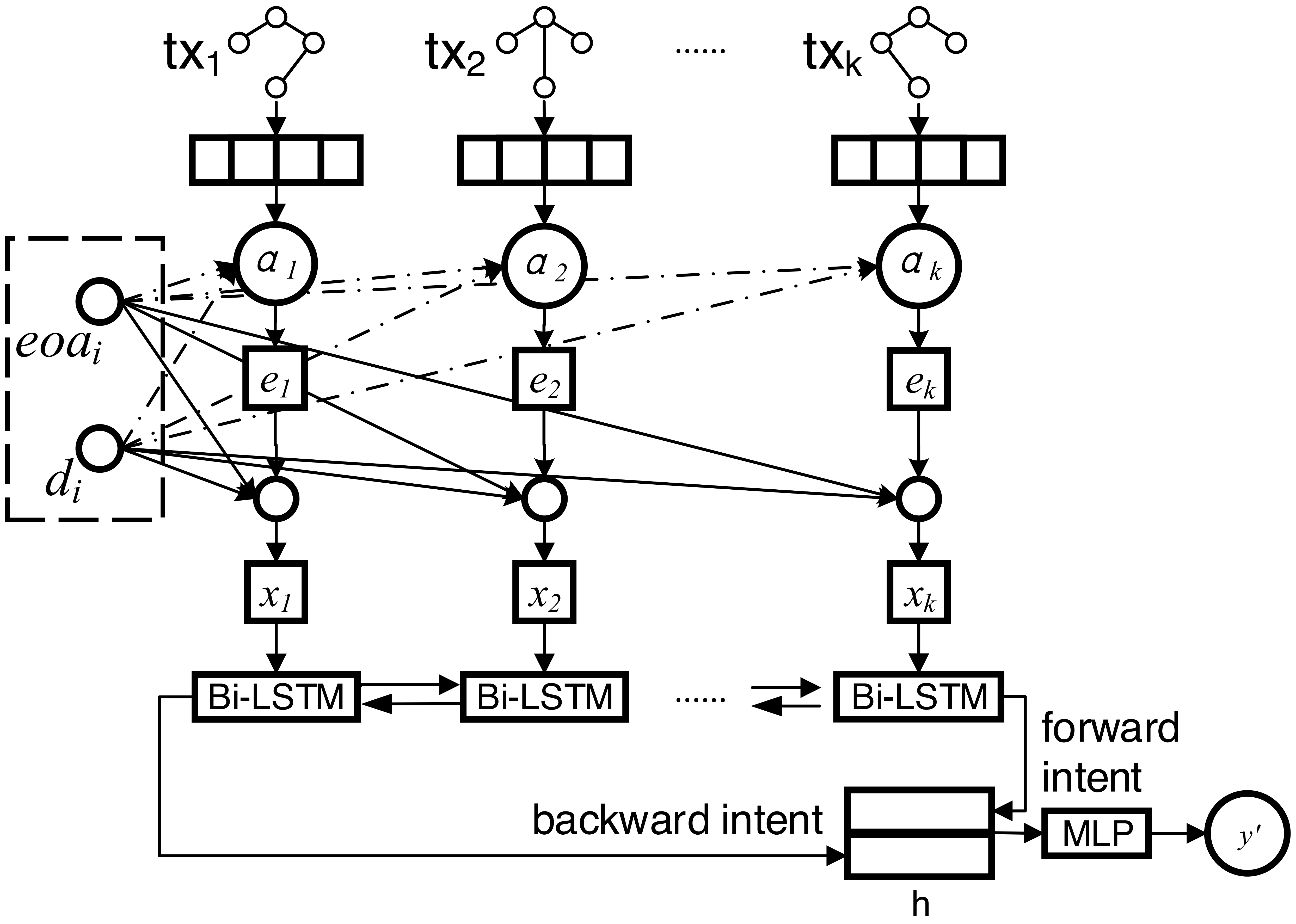


Figure 6: Sequence representation.

Preprocessing

Sequence-based Classification

DEFIER: Idea and Design

Preprocessing

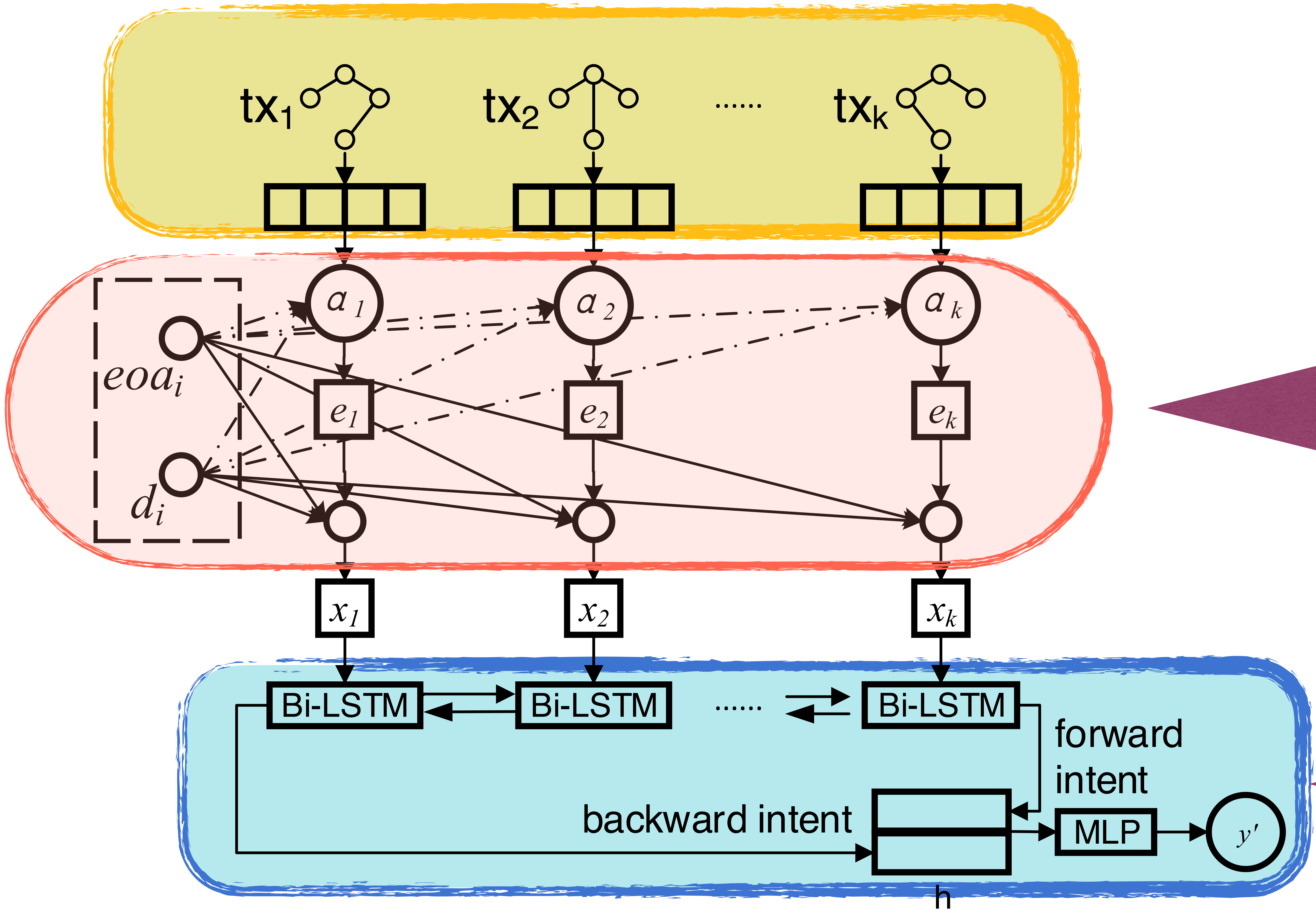
Transaction clustering

$$D(g_1, g_2) = \alpha \boxed{\min_{(o_1,\dots,o_k)\in O(g_1,g_2)} \sum_{i=1}^{k} c(o_i)} + \boxed{\beta \Delta t} \qquad (1)$$

- Structure similarity
- Timing closeness

DEFIER: Idea and Design

Sequence-based Classification



EOA-Dapp-execution attention model: highlight the useful information related to the EOA's intent on the Dapp.

Output types: normal, preparation, exploitation, propagation and completion.

Discussing the Result

Table 6: Dataset and evaluation results.

Dataset	# transactions	Results
Groundtruth set	badset 57,855 goodset 39,124	pre_{micro} 98.2%, pre_{macro} 92.4% rec_{micro} 98.1%, rec_{macro} 98.4%
Unknown set	2,350,779	$positive$ 476,334
Sampled testset	30,888	pre_{micro} 91.7%
		pre_{macro} 83.6%

pre_{micro} and pre_{macro}: micro of precision, macro of precision
rec_{micro} and rec_{macro}: micro of recall, macro of recall
$positive$: transactions that labeled as one of attack stages

Discussing the Result

Table 10: Victim Dapps in different categories.

Type	# Dapps/0-day	# attacker EOAs/0-day	# exploit transactions/0-day	ex. of victim Dapps
Gambling	51/43	65,778 /11,339	360,524 /114,473	Lucky Blocks
Game	28/27	959/919	52,673 /52,176	SpaceWar
Finance	5/5	183/183	59,872 /59,872	STOX
Token	2/1	279/167	4,478/472	Power of Bubble
Total	85/75	67,199 /12,608	476,342 /226,763	

Table 11: Unknown set result.

Attack stage	# Dapps/0-day	# attacker EOAs/0-day	# exploit transactions/0-day
Attack preparation	80/70	42,661/8,237	214,408/106,436
Exploitation	85/75	35,955/3,650	143,179/39,908
Attack propagation	75/65	18,466/6,545	118,755/80,419

Summary

The **first measurement study** and forensic analysis on real-world Dapp attacks.

Our new understanding and CTI discovered can **help mitigate the threat to Dapps.**

Discover **476,342 exploit transactions** on **85 target** (with a microprecision of 91.7%).

DEFIER reported **75 0-day victim Dapps**.

An attack lifecycle discovery tool can potentially be used to disrupt exploits, sometimes even before damages are inflicted.

Thank you!

Authors:

Liya Su, Xinyue Shen, Xiangyu Du, Xiaojing Liao
XiaoFeng Wang, Luyi Xing, Baoxu Liu

Contact:

suliya@iie.ac.cn

Availability:

The annotated data and the implementation of DEFIER is available at *https://drive.google.com/drive/folders /1cdD1gHNbWIS228QXmeUReougSL_k1kvf?usp=sharing*.