32ND USENIX Security Symposium

BLOCKCHAIN

THE IMITATION GAME

Kaihua Qin, Stefanos Chaliasos, Liyi Zhou, Benjamin Livshits, Dawn Song, Arthur Gervais
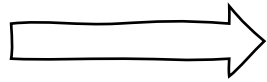
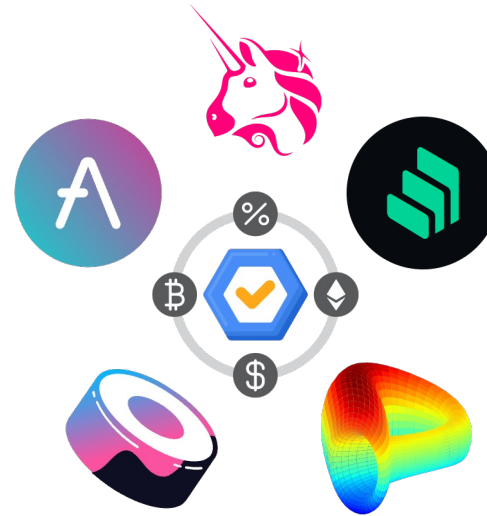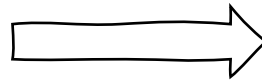Imperial College London   Berkeley UNIVERSITY OF CALIFORNIA   UCL

Decentralized Finance

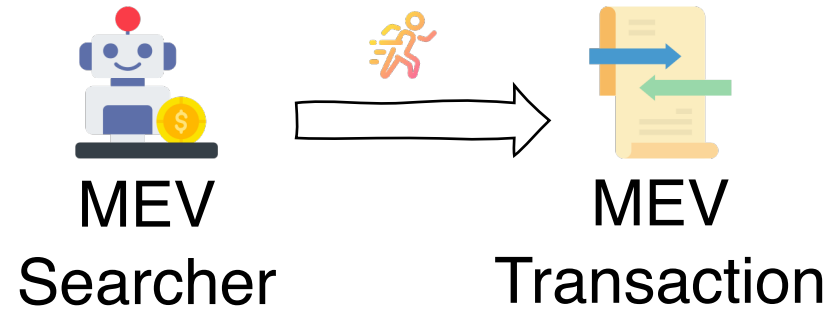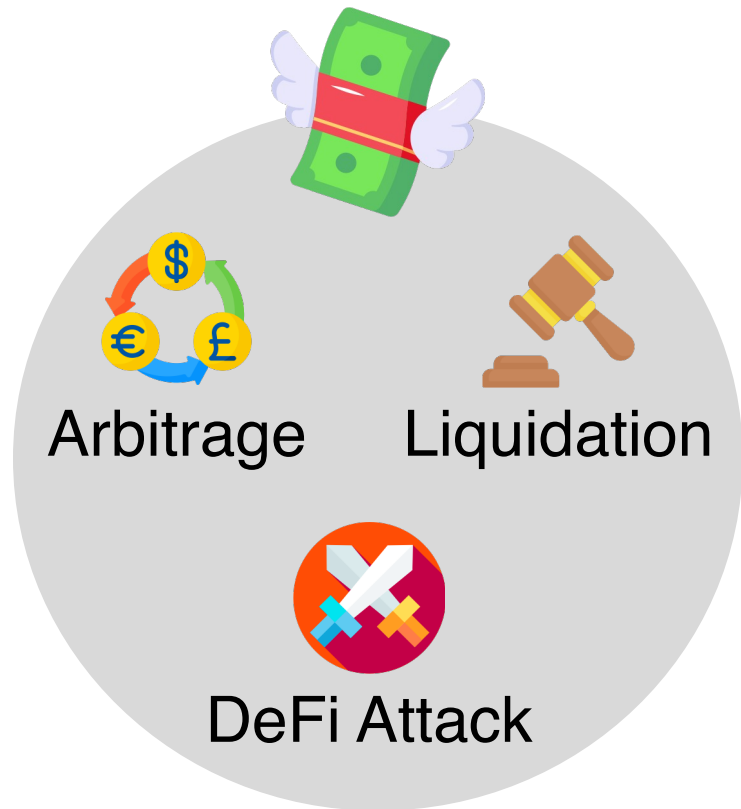Bitcoin → Ethereum → Decentralized Finance (DeFi)

MEV

Arbitrage Liquidation

DeFi Attack

MEV
Searcher

MEV
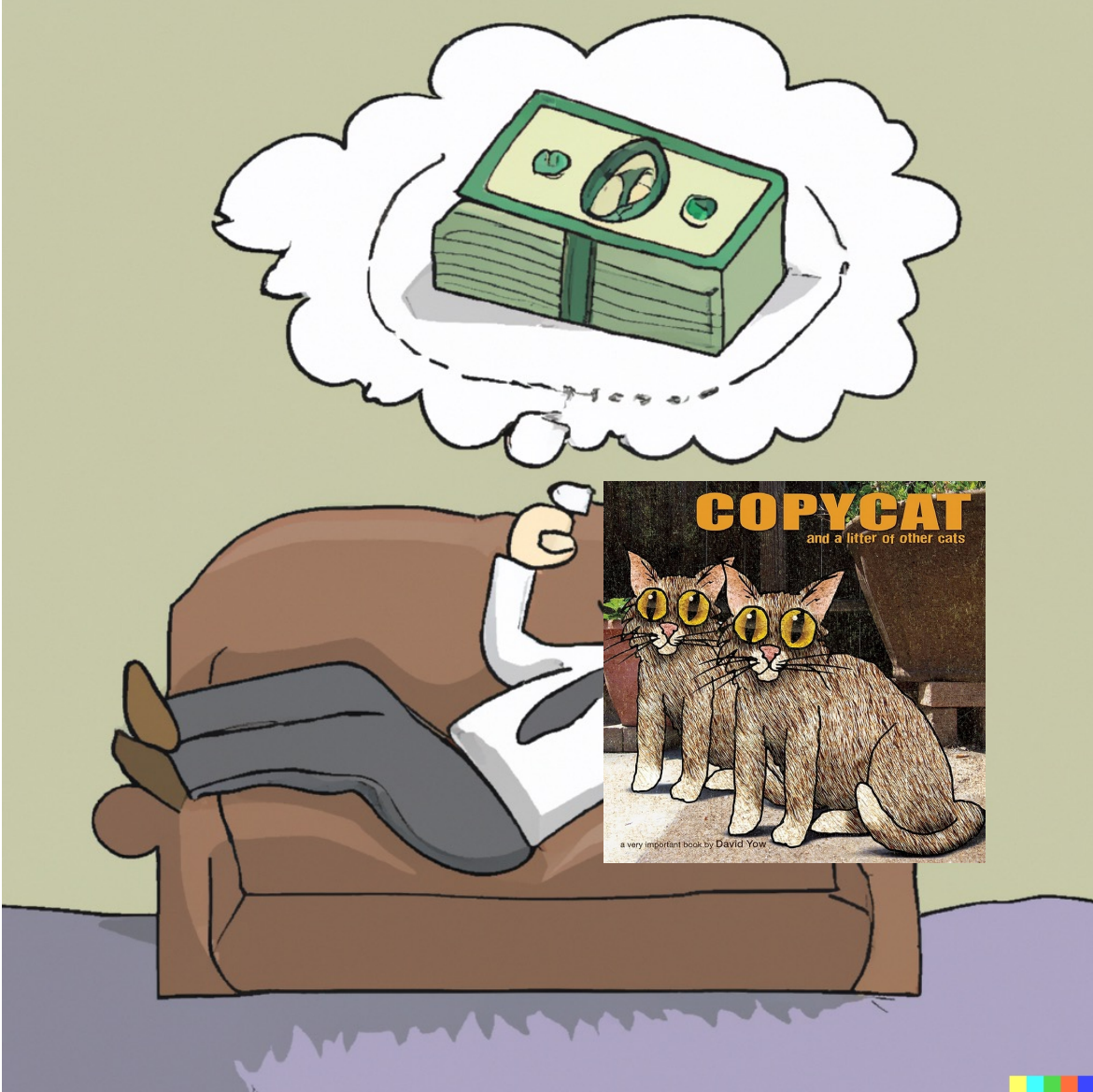Transaction

```
contract MEV {

    function arb() public {

        swapETHtoUSDC();

        swapUSDCtoETH();

        msg.sender.transfer(profit);
    }
}
```

The Blockchain Imitation Game

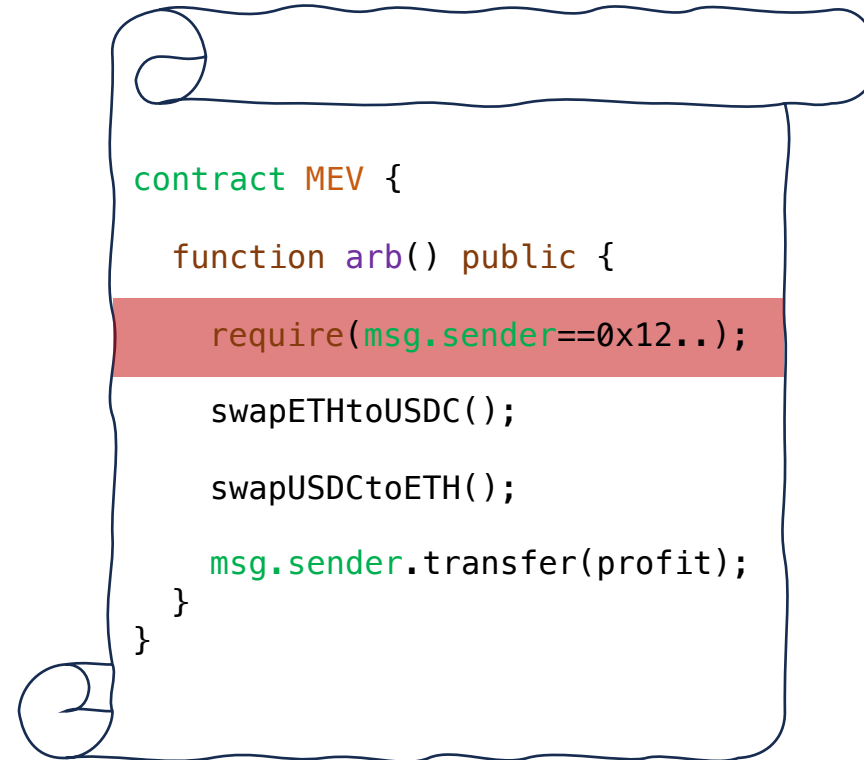# Imitation

Creation → Observation → Execution

Copy-paste

Front-run

Naive Imitation

- String replacement

- Simple but effective

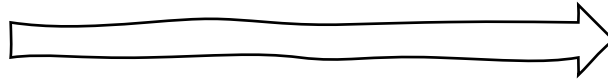- 35M USD (December 2018 – August 2021) on Ethereum

- Easy to prevent

```
contract MEV {

    function arb() public {

        require(msg.sender==0x12..);

        swapETHtoUSDC();

        swapUSDCtoETH();

        msg.sender.transfer(profit);
    }
}
```

Qin, K., Zhou, L., & Gervais, A. Quantifying blockchain extractable value: How dark is the forest?.
In 2022 IEEE Symposium on Security and Privacy (SP).
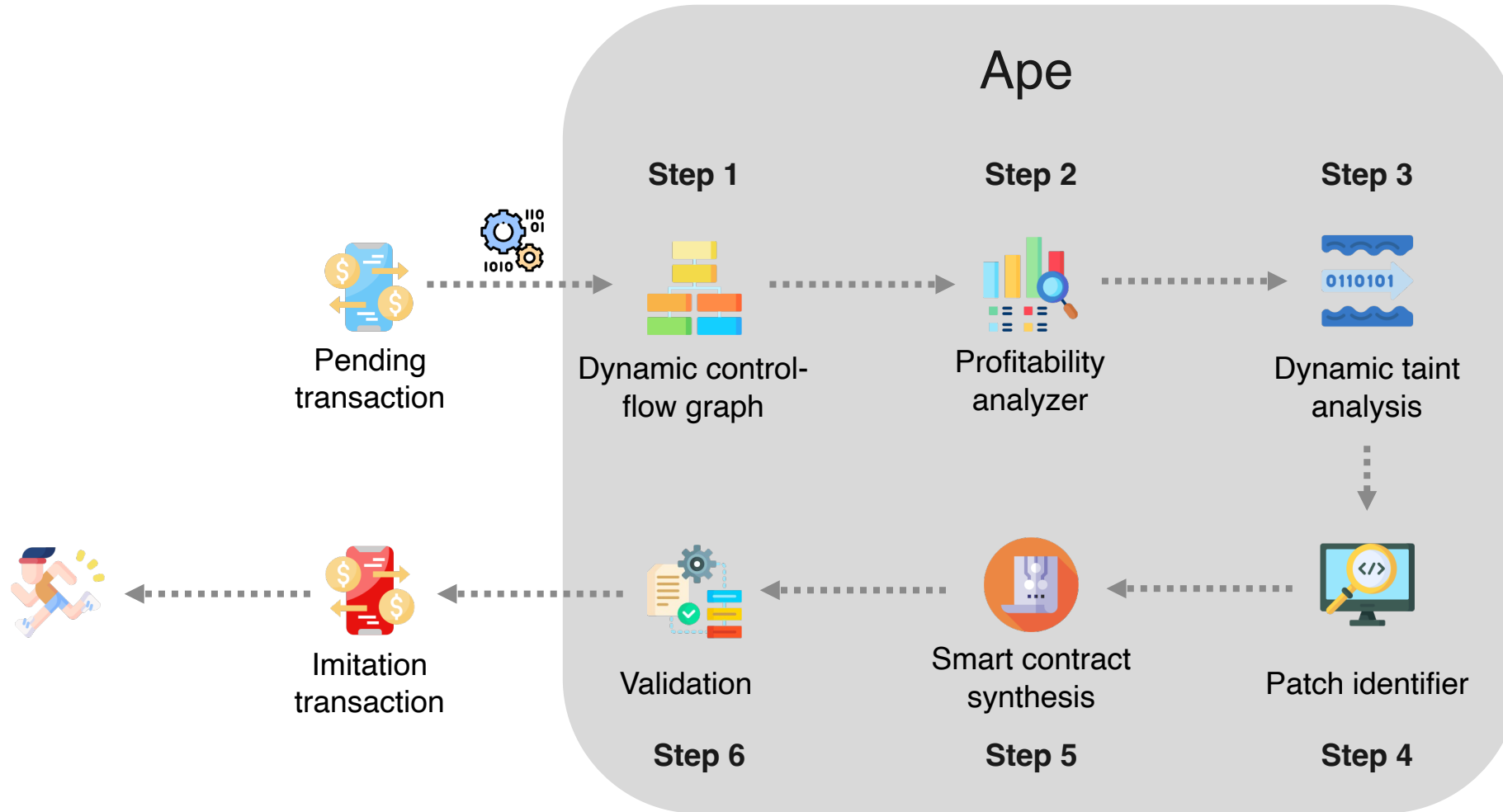
Ape — Generalized Imitation


```
contract MEV {

  function arb() public {

    require(msg.sender==0x12..);

    swapETHtoUSDC();

    swapUSDCtoETH();

    msg.sender.transfer(profit);
  }
}
```

Imitate & Synthesize →

```
contract MEV {

  function arb() public {

    require(msg.sender==0x12..);

    swapETHtoUSDC();

    swapUSDCtoETH();

    msg.sender.transfer(profit);
  }
}
```

Methodology Overview

Evaluation

August 1, 2021 – July 31, 2022 (1 year)   0.07 second
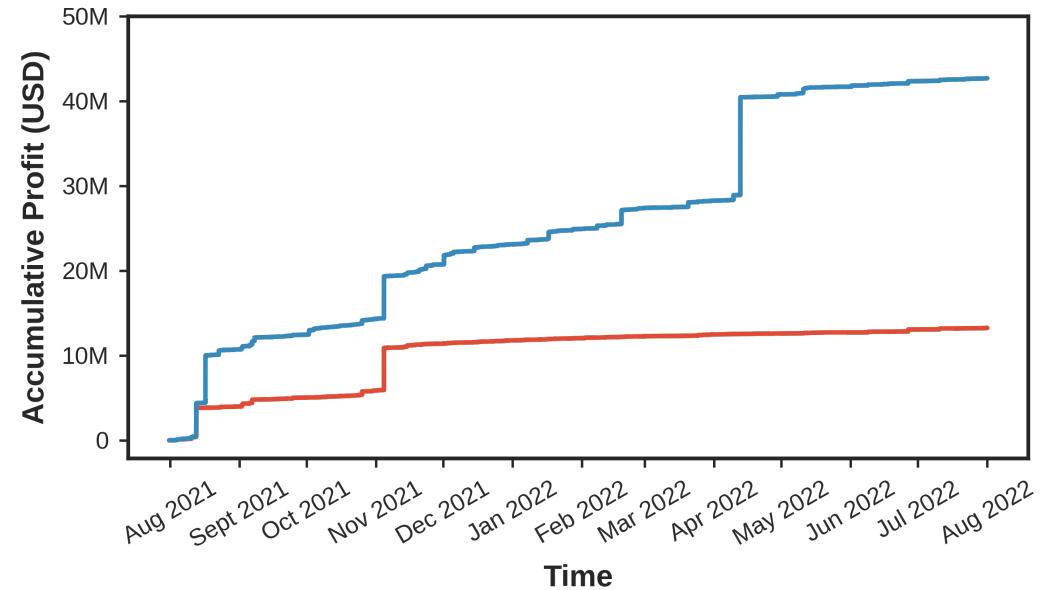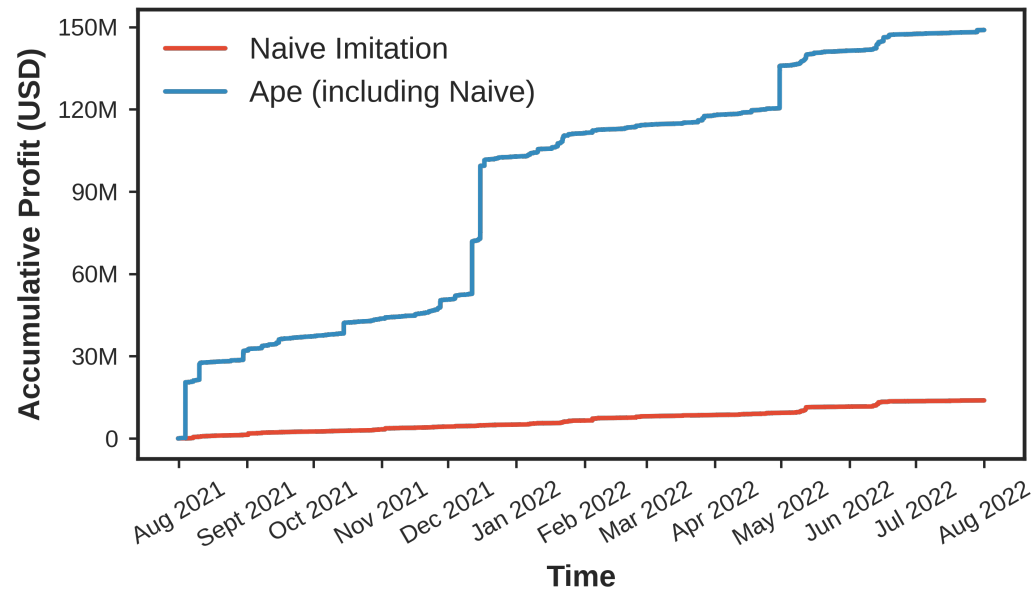
Ethereum   💰 148.96M USD   BSC   💰 42.70M USD

Imitation as Whitehat

DeFi Attacks

Ethereum

29   73.74M USD

BSC

40   22.39M USD

Protocol	Loss (USD)	Date
Popsicle Finance	20.25M	Aug-03-2021
Saddle Finance	9.71M	Apr-30-2022
Indexed Finance	3.58M	Oct-14-2021
…	…	…

Protocol	Loss (USD)	Date
Elephant Money	11.52M	Apr-12-2022
XSURGE	5.17M	Aug-16-2021
CollectCoin	1.06M	Dec-01-2021
…	…	…

Questions

Kaihua Qin

https://qin.ac/