

# Take The Money And Run

## Decentralized Finance and the New Frontiers of Crime

Giovanni Vigna

UCSB



SECLAB

# \$whoami

- Computer Science Professor at UC Santa Barbara
- Co-founder CTO at Lastline, Inc. (acquired by VMware in 2020)
- Sr. Director of Threat Intelligence at VMware
- Founder of Shellphish



# What Is DeFi?

“Decentralized finance offers financial instruments without relying on intermediaries such as brokerages, exchanges, or banks by using smart contracts on a blockchain”

- Wikipedia

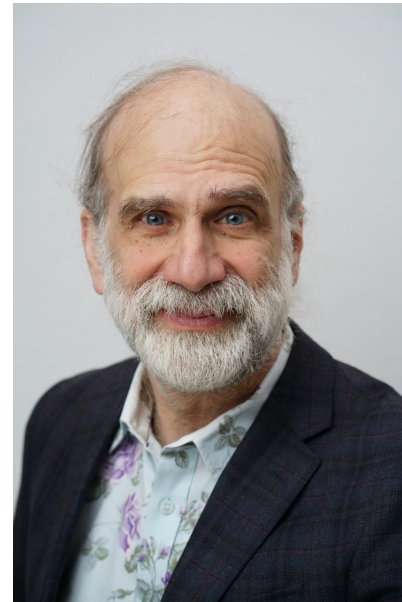
# Enthusiasts



- Provides unfettered access to financial instruments
- Takes out the middleman
- Takes away centralized control
- Uses code as the law
- It's transparent
- It's cheap(er)

# Detractors

- It's a scam that hurts people
- Transactions are irreversible
- Its value is not backed by a real economy
- It is not really decentralized
- It still has middlemen
- Most of its transactions are speculation and scams
- It's bad for the environment



# Letter in Support of Responsible Fintech Policy

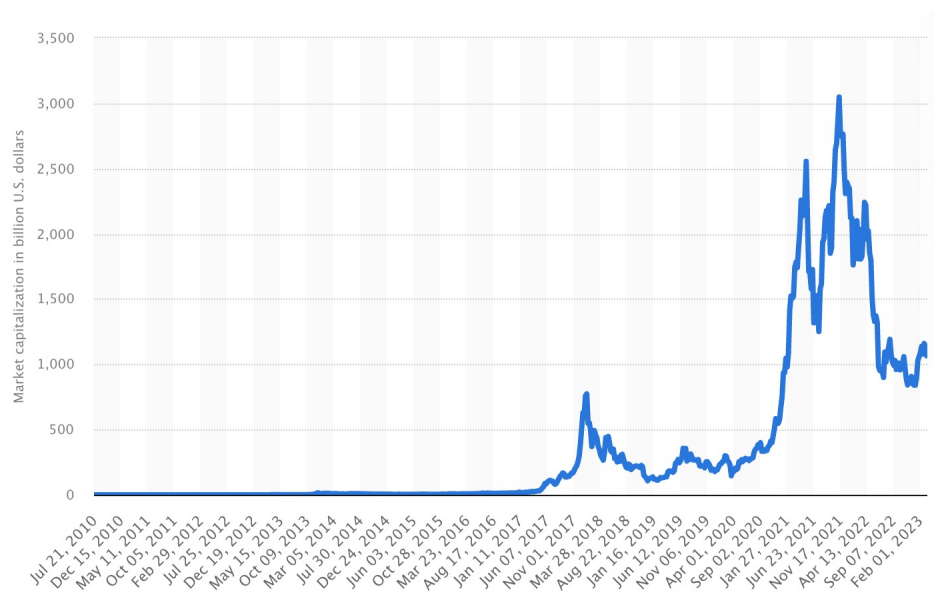
“...we write to you urging you to take a critical, skeptical approach toward industry claims that crypto-assets (sometimes called cryptocurrencies, crypto tokens, or web3) are an innovative technology that is unreservedly good. We urge you to resist pressure from digital asset industry financiers, lobbyists, and boosters to create a regulatory safe haven for these risky, flawed, and unproven digital financial instruments and to instead take an approach that protects the public interest and ensures technology is deployed in genuine service to the needs of ordinary citizens”

<https://concerned.tech/>

# A Wild Ride

LONDON, June 13 (Reuters) - The value of the cryptocurrency market on Monday fell below \$1 trillion for the first time since January 2021, according to data site CoinMarketCap, reaching as low as \$926 billion.

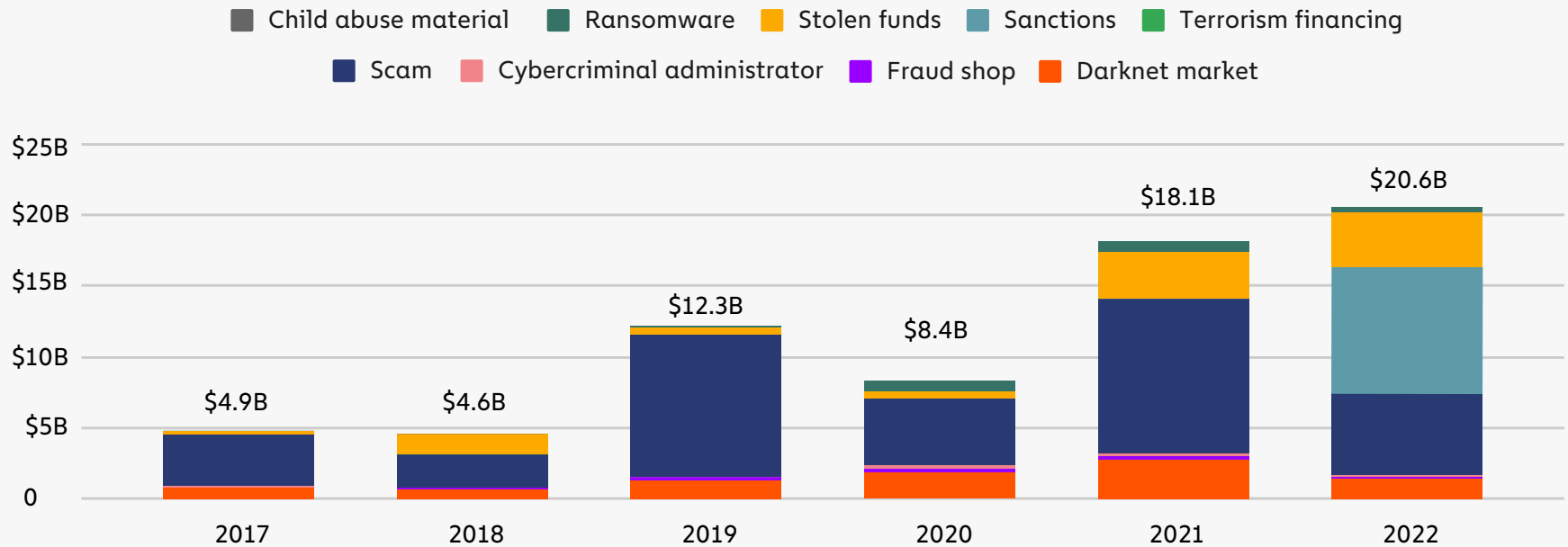
The global cryptocurrency market peaked at \$2.9 trillion in November 2021, but it has faltered so far this year. It has lost \$1 trillion in value in the last two months alone as investors ditched riskier assets in the face of high inflation and fears that interest rate raises by central banks will hamper growth.



<https://www.statista.com/statistics/730876/cryptocurrency-maket-value/>

# Illicit Activity

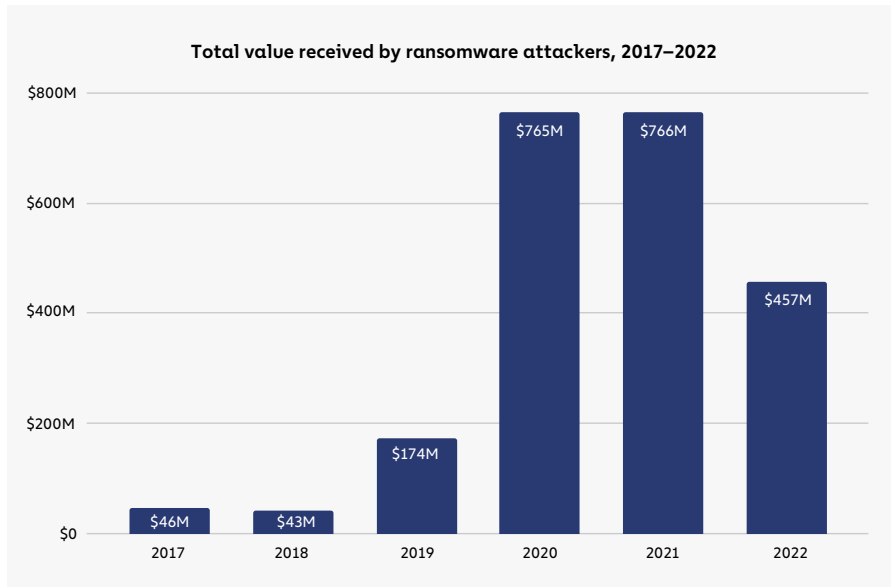
Total cryptocurrency value received by illicit addresses, 2017 - 2022



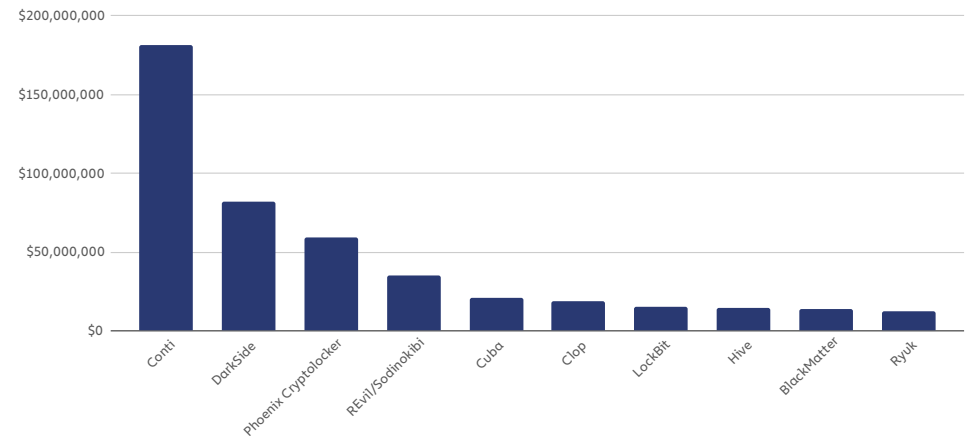
<https://go.chainalysis.com/2023-crypto-crime-report.html>



# Ransomware



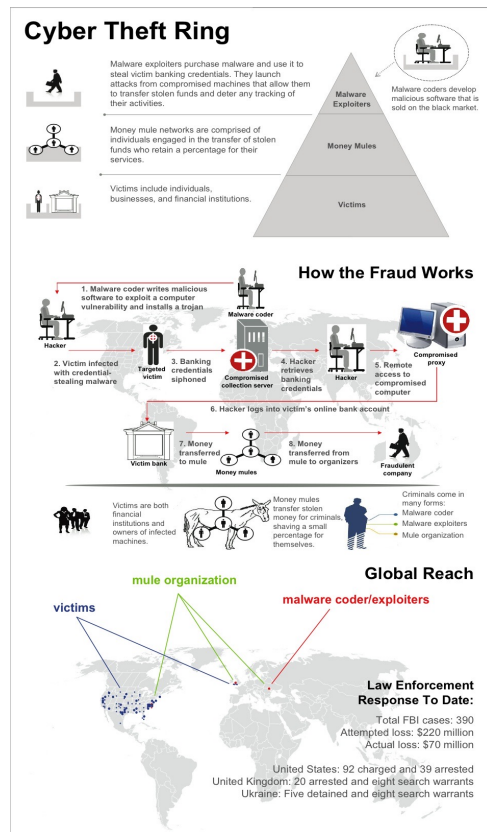
**Top 10 ransomware strains by revenue | 2021**



<https://go.chainalysis.com/2022-Crypto-Crime-Report.html>

<https://go.chainalysis.com/2023-crypto-crime-report.html>

# Compare to the Good Ol' Days...



- Zeus: 2007-2010
- “More than 100 people were arrested on charges of conspiracy to commit bank fraud and money laundering, over 90 in the US, and the others in the UK and Ukraine. Members of the ring had stolen \$70 million.”

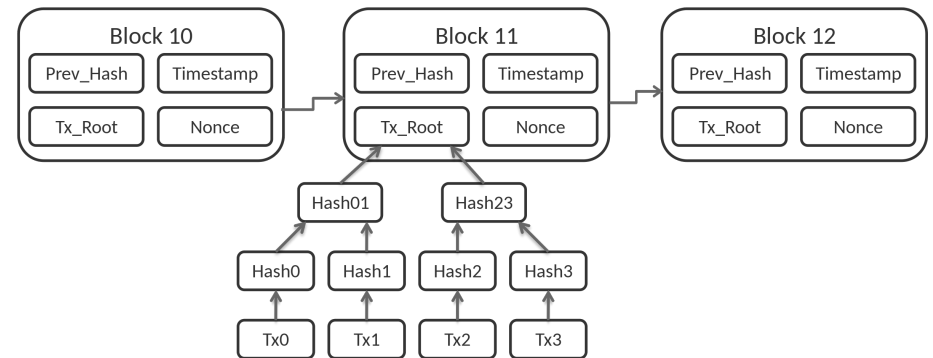
[https://en.wikipedia.org/wiki/Zeus\\_\(malware\)](https://en.wikipedia.org/wiki/Zeus_(malware))

**We Need to Talk About the  
Blockchain..**













# Blockchains, Blocks, and Transactions

- Append-only distributed security ledgers
- Consensus protocol allows for agreement about the contents of the blocks
- Most of the times, the contents of the block are a list of transactions



# L1 Blockchains (and their coins)

Layer-1 coins	Price	Market cap
1  Bitcoin BTC	\$ 28,200.64	\$ 541.96 billion
2  Ethereum ETH	\$ 1,801.56	\$ 219.81 billion
3  BNB BNB	\$ 314.35	\$ 44.93 billion
4  XRP XRP	\$ 0.5281	\$ 26.55 billion
5  Cardano ADA	\$ 0.3826	\$ 13.40 billion
6  Dogecoin DOGE	\$ 0.08013	\$ 10.96 billion
7  OKB OKB	\$ 41.37	\$ 9.99 billion
8  Polkadot DOT	\$ 6.326	\$ 7.67 billion
9  Solana SOL	\$ 20.63	\$ 7.49 billion
10  Litecoin LTC	\$ 92.95	\$ 6.59 billion

- Bitcoin and Ethereum account for the vast majority of the market cap
- Ethereum
  - Supports smart contracts
  - In September 2022, moved from Proof-of-Work to Proof-of-Stake

<https://coinranking.com/coins/layer-1>

# Smart Contracts

- Programs running on top of Ethereum blockchain
- Execute as bytecode on top of Ethereum Virtual Machine (EVM)
- Typically developed in higher-level languages such as Solidity
- Power DeFi applications, tokens, games, collectibles, ...

# Ethereum Transactions

- Transfer Ether from address A to address B
  - Deploy a smart contract on the block chain
  - Invoke a function in a deployed smart contract
- 
- Transactions are submitted to a public mempool
  - There are ways to bypass the mempool by using Flashbots



# Block Producers and MEV





- Block Producers: Miners (PoW) and Validators (PoS)
- “Maximal Extractable Value (MEV) refers to the maximum value that can be extracted from block production in excess of the standard block reward and gas fees by including, excluding, and changing the order of transactions in a block.”  
(<https://ethereum.org/en/developers/docs/mev/>)
- Bots and producers compete to determine the selection and ordering of transaction in a block
- Typical example: Arbitrage (more on that later)

# Tokens

- Token contracts are used to track ownership of assets
- ERC-20 standardizes the interface for fungible token contracts
- ERC-721 standardizes the interface for non-fungible token contracts

Token Tracker (ERC-20)











A total of 1,211 Token Contracts found

#	Token	Price	Change (%)	Volume (24H)	Circulating Market Cap	On-Chain Market Cap	Holders
1	 Tether USD (USDT)	\$1.001 0.000535 ETH	▲ 0.03%	\$22,693,337,496.00	\$80,156,488,012.00	\$39,862,942,964.85	4,225,728 0.097%
2	 BNB (BNB)	\$312.5114 0.167061 ETH	▼ -0.63%	\$530,114,321.00	\$49,341,545,270.00	\$5,181,288,081.31	279,522 0.013%
3	 USD Coin (USDC)	\$1.00 0.000535 ETH	▲ 0.03%	\$3,771,726,900.00	\$32,769,067,004.00	\$46,602,430,840.00	1,641,465 0.232%
4	 HEX (HEX)	\$0.0703 0.000038 ETH	▼ -13.81%	\$14,146,388.00	\$12,193,718,103.00	\$40,612,736,110.50	330,298 0.006%

<https://etherscan.io/tokens>

# Centralized Exchanges

- Ramp-in
  - Transfer money from a bank account into Ether
- Ramp-out
  - Transfer Ether into actual money in a bank account

# ▲	Exchange	Score ⓘ	Trading volume(24h)	Avg. Liquidity	Weekly Visits ⓘ	# Markets	# Coins	Fiat Supported
1	 Binance 	9.9	\$6,623,164,743 ▼ 9.33%	832	14,280,411	1688	384	EUR, GBP, BRL and +8 more ⓘ
2	 Coinbase Exchange 	8.1	\$572,601,133 ▼ 29.87%	715	43,888	598	237	USD, EUR, GBP
3	 Kraken 	7.8	\$226,473,781 ▼ 28.96%	738	1,050,071	709	224	USD, EUR, GBP and +4 more ⓘ
4	 KuCoin 	7.2	\$543,527,316 ▼ 6.66%	528	2,124,343	1448	815	USD, AED, ARS and +45 more ⓘ
5	 Bitfinex 	6.9	\$60,770,819 ▼ 11.33%	604	698,833	408	187	USD, EUR, GBP and +1 more ⓘ

<https://coinmarketcap.com/rankings/exchanges/>

# Where's the Money?

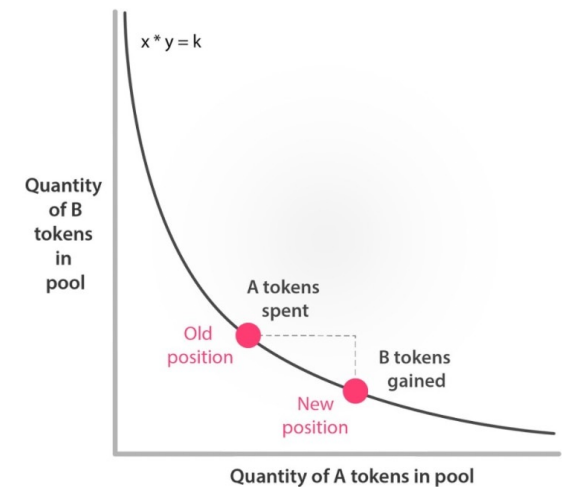


# Make the Money

- Lending (Flash loans!)
  - AAVE, Compound
- Derivatives
  - dYdX
- Yield Farms
  - Curve
- Decentralize Exchanges
  - UniSwap, SushiSwap

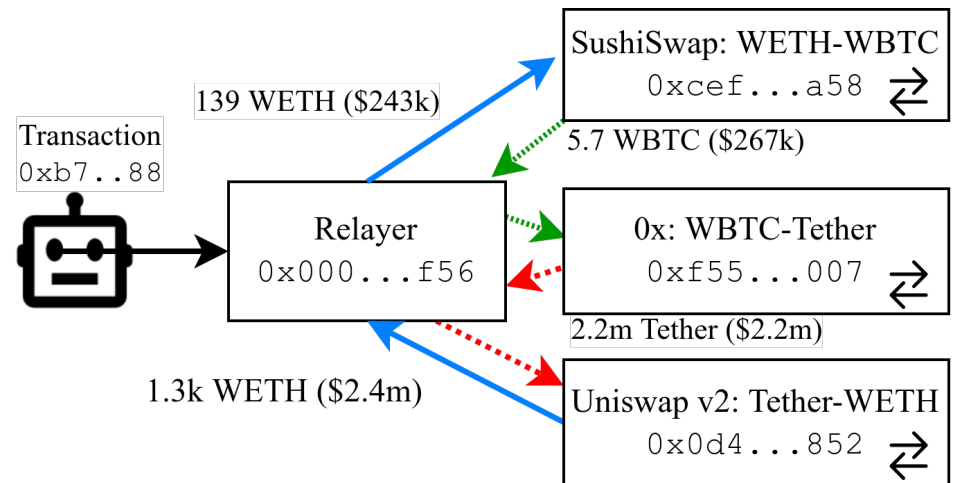
# Automated Market Makers (AMMs)

- Based on liquidity pools
  - They do not maintain an order book
- Exchange price is automatically determined
  - For example, the product of the two assets constant
- Created from smart contract factory



# Arbitrage

- Opportunity caused by the same asset having different prices on different exchanges
- Multiple exchanges in a single transaction
- Analysis performed off-line
- Execution by relayer smart contract



# How Much Arbitrage?

- We analyzed 28 months of data (~1 billion transactions)
- Identified 4,070,938 arbitrage transactions
  - 90+% only 2-3 exchanges involved
  - 90+% pivoted on Wrapped ETH
  - Uniswap v2 and v3 and SushiSwap are the most involved AMMs
- \$321 millions in profit
  - Top bot 1: \$37M
  - Top bot 2: \$31M
  - Top bot 3: \$26M

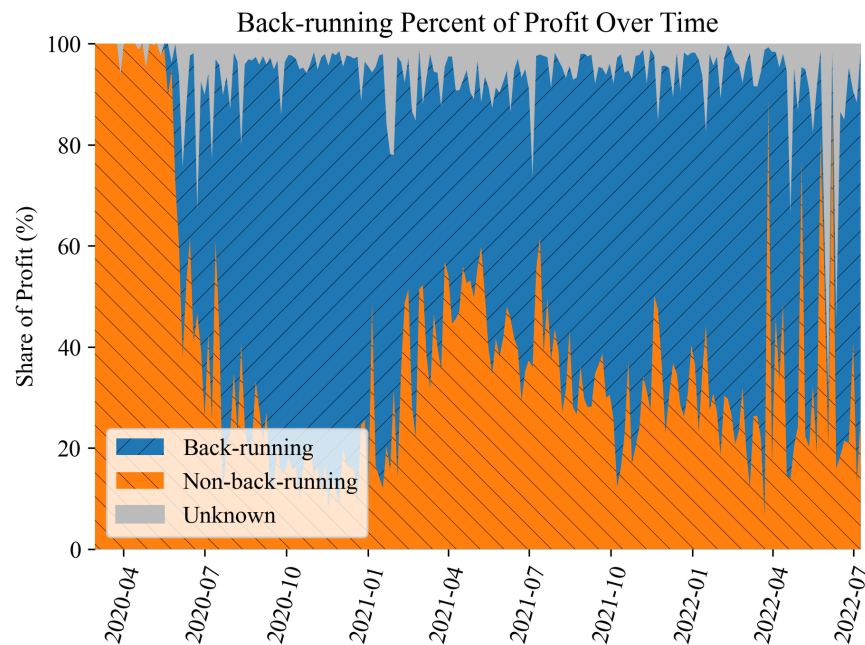
## **A Large Scale Study of the Ethereum Arbitrage Ecosystem**

Robert McLaughlin, Christopher Kruegel, Giovanni Vigna  
*University of California, Santa Barbara*  
*{robert349, chris, vigna}@cs.ucsb.edu*

*USENIX Security 2023*



# Transaction Order Matters



- Bots monitor the mempool
- Identify transactions that might create an arbitrage opportunity
- Attempt to put an arbitrage transaction right after trade (back-running)
- Might use Flashbots to avoid a bidding war

# Transaction Order Matters

- Sandwich attacks
  - Identify a target transaction that might change the valuation of an asset
  - Attempt to put a transaction before and one afterwards to take advantage of the change
- Front-running attacks
  - Identify a profit-making transaction
  - Attempt to put a similar transaction (with a different beneficiary) before the target transaction

# Take the Money

- Stolen funds
  - Hacks
  - Wallet compromise
- Scams
  - Ponzi schemes
  - Pig butchering/romance scams
  - Investment scams
- Ransomware
- Rag pulls

# Hacks! Hacks!

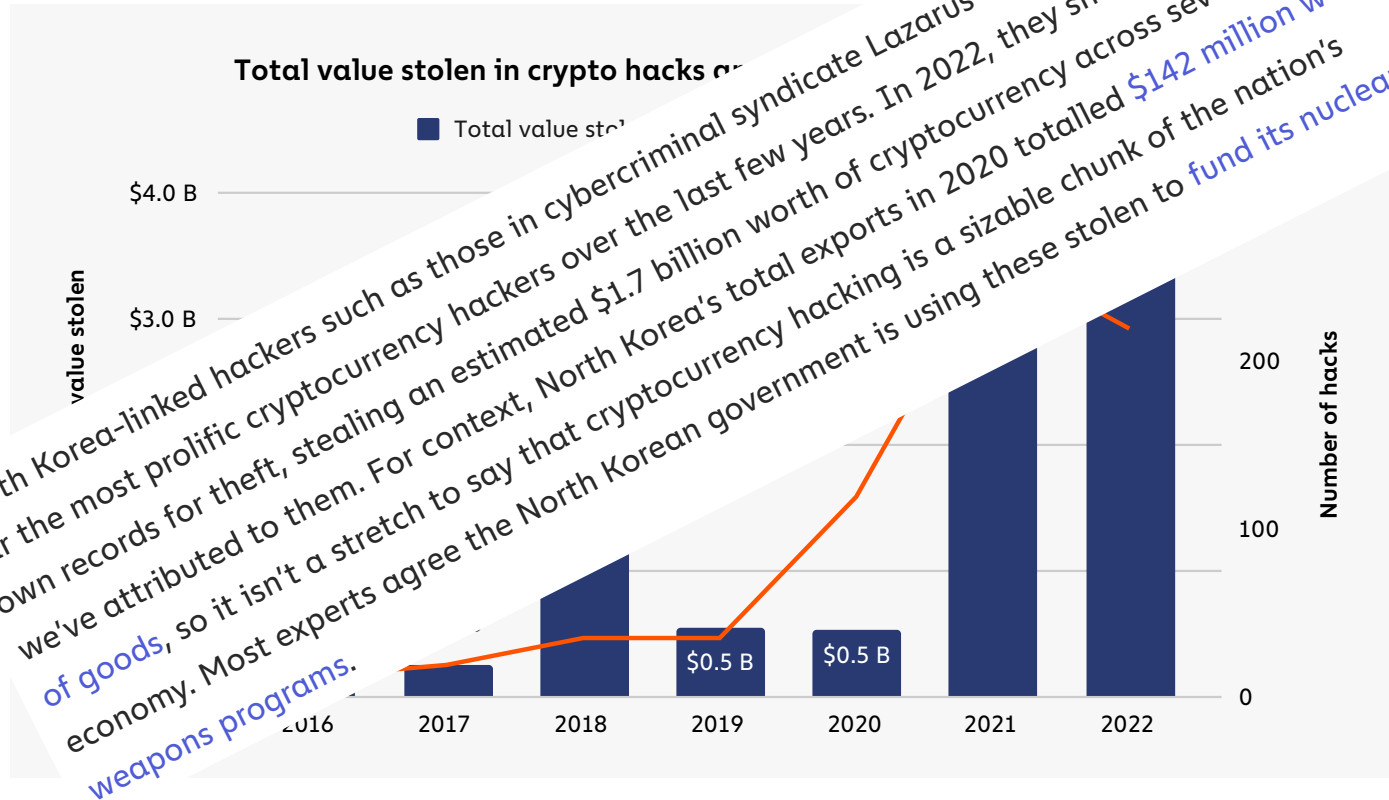
- Traditional hacks
  - Compromised credentials
  - Unauthorized access
- Bridge hacks
  - Custodian attacks
  - Debt issuer attacks
  - Communicator attacks
- Protocol hacks
  - Oracle manipulation
  - ...



- 
1. **Ronin Network** - REKT *Unaudited*  
\$624,000,000 | 03/23/2022
  2. **Poly Network** - REKT *Unaudited*  
\$611,000,000 | 08/10/2021
  3. **BNB Bridge** - REKT *Unaudited*  
\$586,000,000 | 10/06/2022
  4. **SBF - MASK OFF** *N/A*  
\$477,000,000 | 11/12/22
  5. **Wormhole** - REKT *Neodyme*  
\$326,000,000 | 02/02/2022
  6. **Euler Finance** - REKT *Sherlock*  
\$197,000,000 | 03/13/2023
  7. **BitMart** - REKT *N/A*  
\$196,000,000 | 12/04/2021
  8. **Nomad Bridge** - REKT *N/A*  
\$190,000,000 | 08/01/2022
  9. **Beanstalk** - REKT *Unaudited*  
\$181,000,000 | 04/17/2022
  10. **Wintermute** - REKT 2 *N/A*  
\$162,300,000 | 09/20/2022

<https://rekt.news/>

# Amount of Stolen Funds



<https://go.chainalysis.com/2023-crypto-crime-report.html>

# Ronin Network Hack

- Side chain
- Required consensus of 5 out of 9 servers for transfer
- 4 servers were managed by the same entity
- A fifth entity had temporarily delegated the right to sign
- The hacker stole \$624M
- The team didn't notice until a week later...

# Nomad Bridge Hack

- Faulty update allows for address 0x0 to be authorized as root
- First attempt to compromise failed (and cost \$350K in gas!)
- Second attempt succeeded and was followed by everyone else
- \$190M stolen in 2.5 hours as a result

<https://defillama.com/protocol/nomad>



# Wormhole Hack

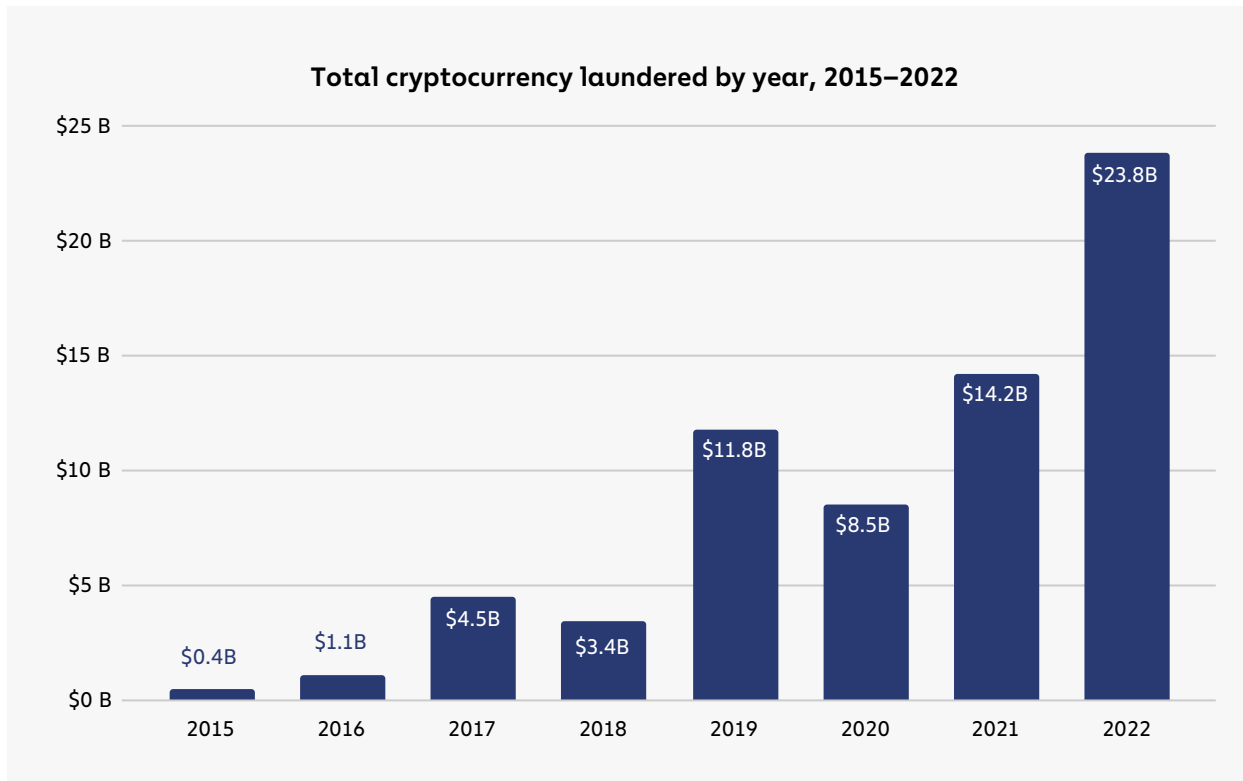
- Wormhole is a token bridge between Ethereum and Solana
- A bug allowed an attacker to provide both a signature and the contract needed to verify the signature
- This allowed for the minting of wrapped Ethereum on Solana, which was then transferred back to Ethereum
- \$326M were lost



# Take the Money and Launder It

- Once the money is stolen, it can be tracked, requiring laundering
- Money can be laundered by mixers, exchanges, DeFi applications, games, etc.
- DeFi applications have seen a substantial increase as a means to launder cash
- Tornado Cash is a mixer that uses Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARKs) to allow a user to deposit an Ether amount and then extract it without the possibility to link the two operations

# Cryptolaundry



<https://go.chainalysis.com/2023-crypto-crime-report.html>

# US Fights Back

- The US Office of Foreign Assets Control (OFAC) has put exchanges (e.g., Russia-based Suex and Chatex, in September 2021) on the Specially Designated Nationals and Blocked Persons (SDN) list
- In May 2022, OFAC put Blender.io on the SDN list
- In August 2022, OFAC put Tornado Cash on the SDN list
  - Used to launder Lazarus group's \$455M heist

# Securing Smart Contracts

- “The code is the law”
- What if the code is broken?
- What if the source code is not even public?
- Problems
  - Function visibility
  - Reentrancy and order of transactions
  - Timing
  - Randomness

# Audits and Bug Bounties

- Ecosystem of companies that perform audits
  - Trail of Bits, ConsenSys Diligence, Certik, Hacken, OpenZeppelin, ...
- Provide no guarantees
- Bug bounties are a way to incentivize responsible disclosure
  - Immunefi, HackenProof



# Automated Vulnerability Analysis

- Combination of static and dynamic analysis
- Small code sizes make it possible to adopt resource-heavy approaches
- Execution is limited by gas price
- Memory models are simpler
- All the code is available

# Reentrancy

```
contract Bank {
    mapping (address => uint) accounts;

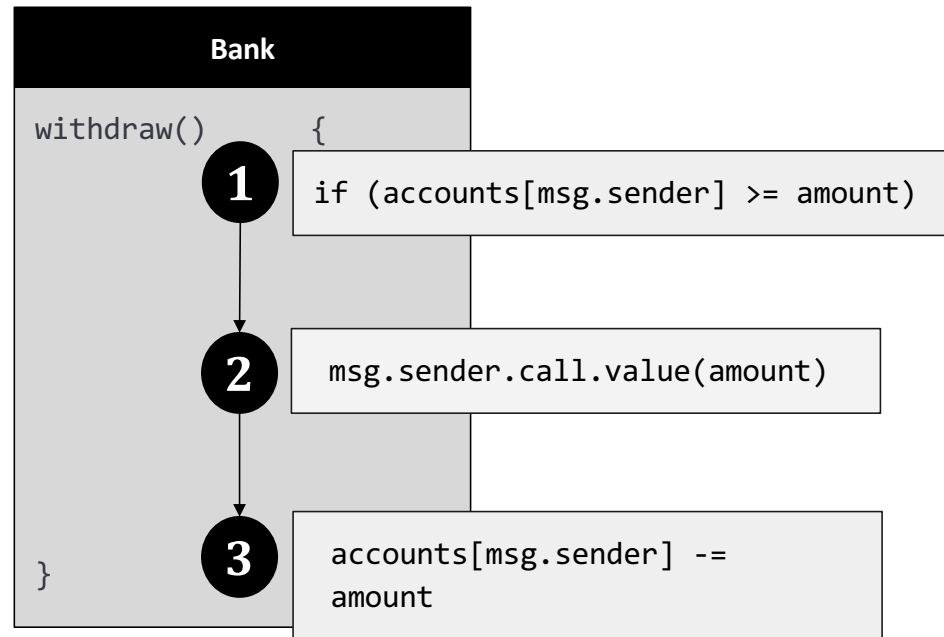
    function withdraw(uint amount) public {
        if (accounts[msg.sender] >= amount) {
            msg.sender.call.value(amount);
            accounts[msg.sender] -= amount;
        }
    }
}
```

```
contract User {
    Bank bank;
    function getEthers() public { bank.withdraw(100);}
    function () public payable { bank.withdraw(100);}
}
```

- Bank contract allows withdrawal of Ethers by users
- The `withdraw()` function transfers the amount through an external call
- After the call returns, user's balance is updated.
- A user implements `getEthers()` to withdraw **100 Ethers** from the Bank
- She also invokes `bank.withdraw(100)` within her `fallback()` function as well

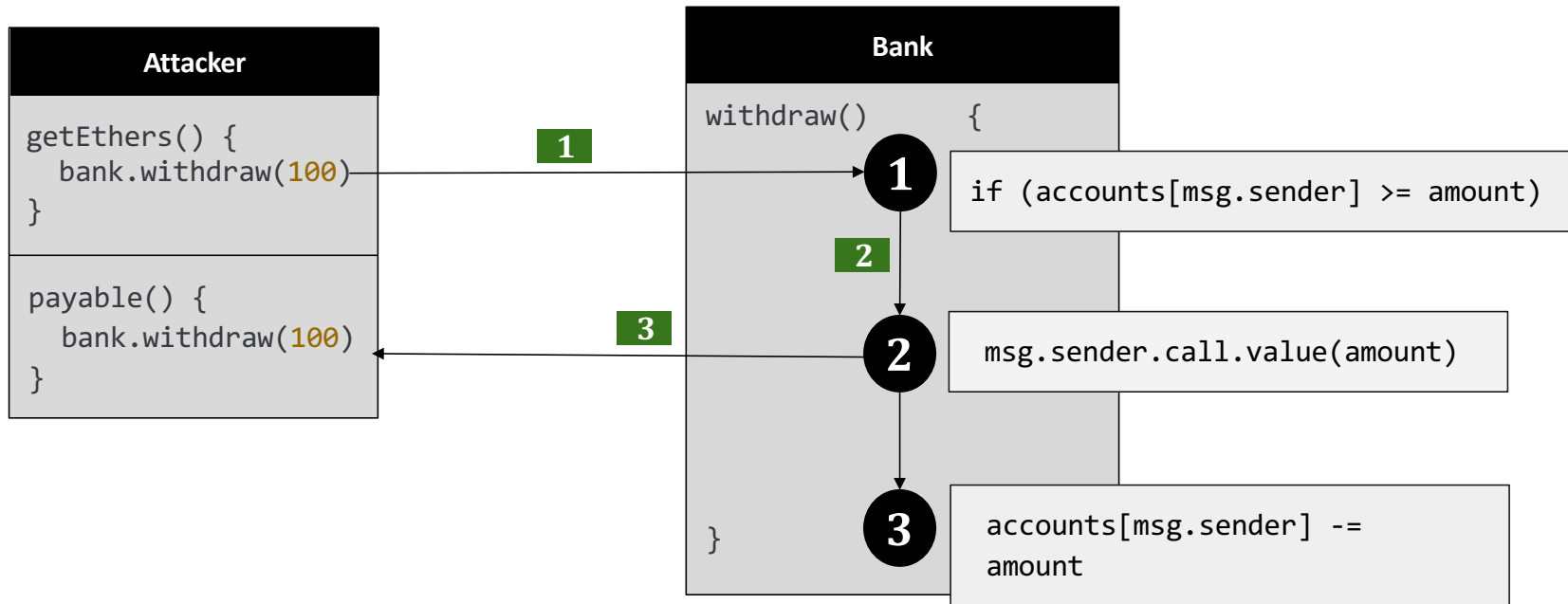
# Reentrancy

Attacker
<pre>getEthers() {   bank.withdraw(100) }</pre>
<pre>payable() {   bank.withdraw(100) }</pre>

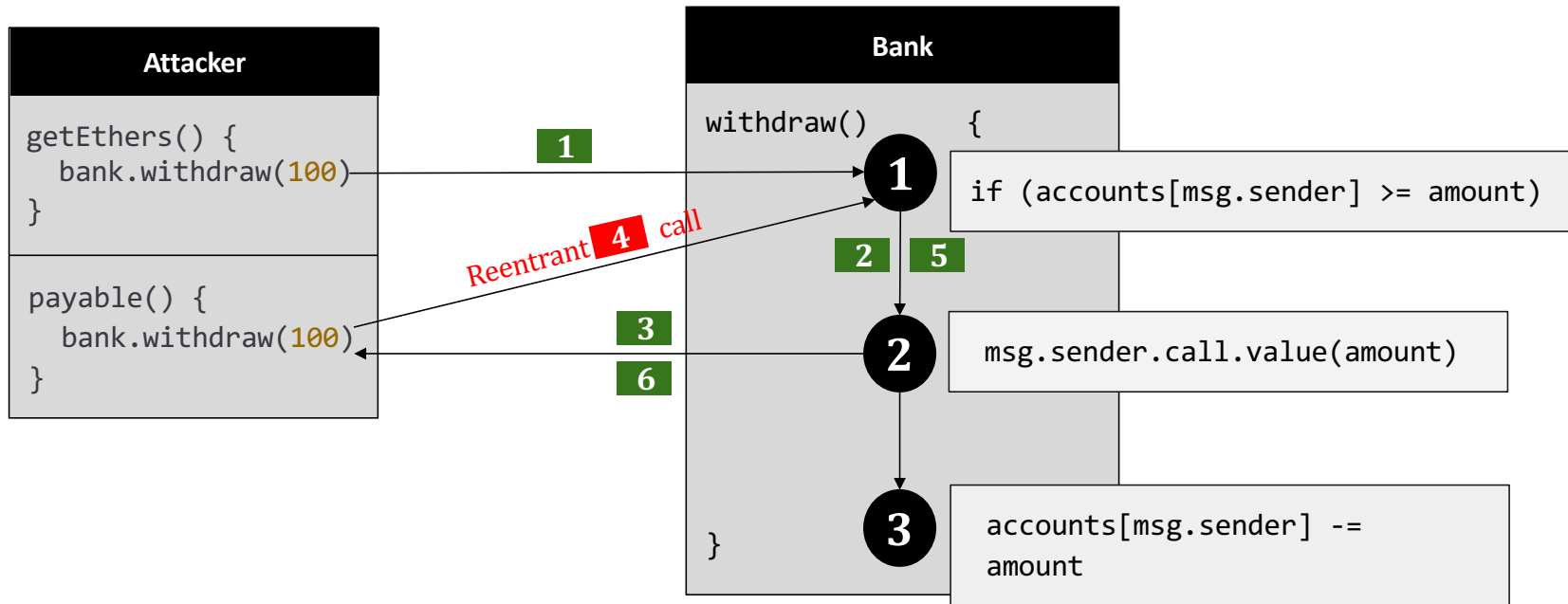




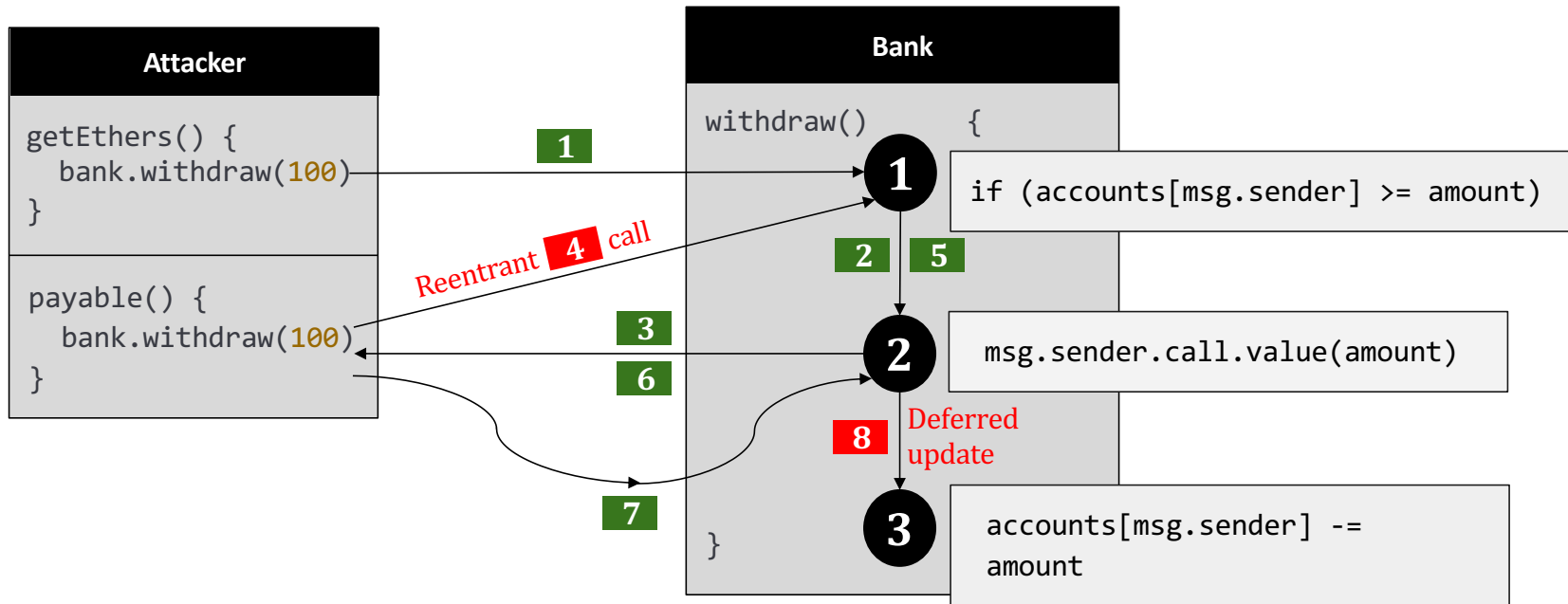
# Reentrancy



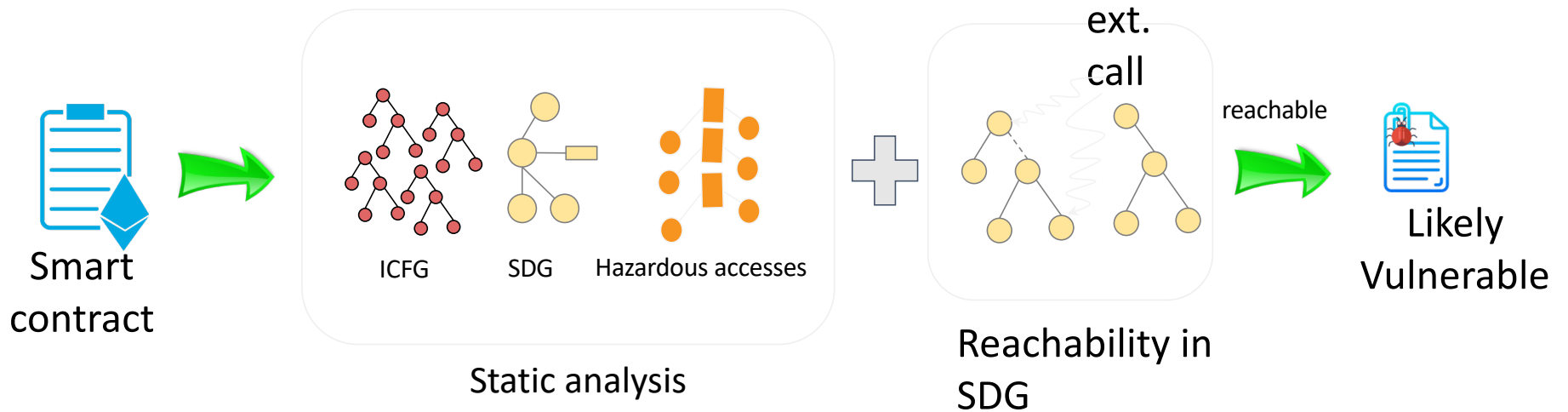
# Reentrancy



# Reentrancy



# Sailfish



## SAILFISH: Vetting Smart Contract State-Inconsistency Bugs in Seconds

Priyanka Bose, Dipanjan Das, Yanju Chen, Yu Feng, Christopher Kruegel, and Giovanni Vigna  
University of California, Santa Barbara  
{priyanka, dipanjan, yanju, yufeng, chris, vigna}@cs.ucsb.edu

*IEEE Symposium on Security and Privacy, May 2022*

# Confused Deputy

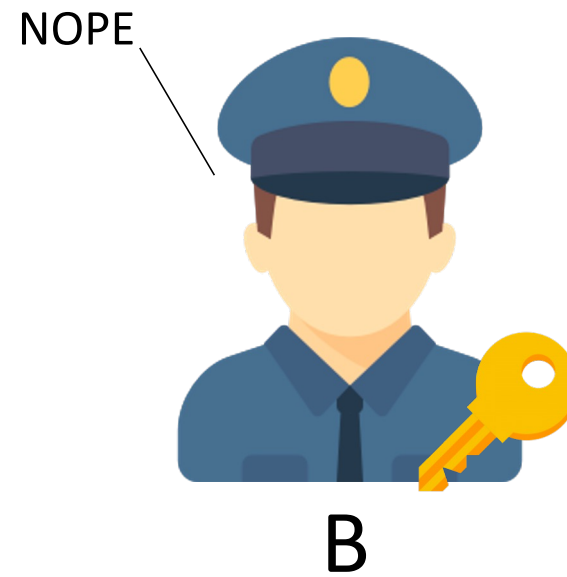
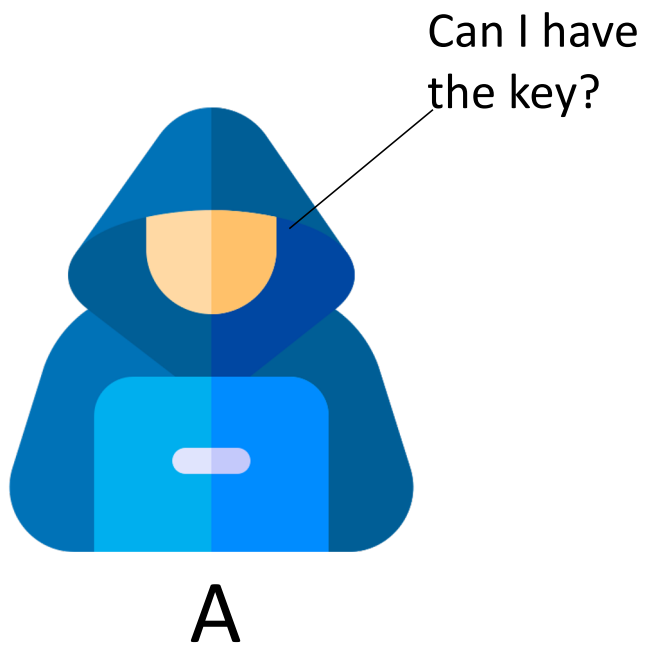


A

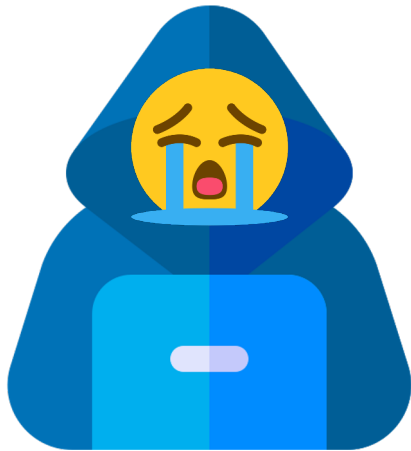


B

# Confused Deputy



# Confused Deputy



A



B

# Confused Deputy



A

Ask for  
the key  
and give it  
to me!



C

B



# Confused Deputy



A



C

I need  
the key!



B

# Confused Deputy



A



C

Oh,  
sure!



B

# Confused Deputy



A



C



B

# Confused Deputy



A

Here the  
key, have a  
nice day!



C



B

# Confused Deputy

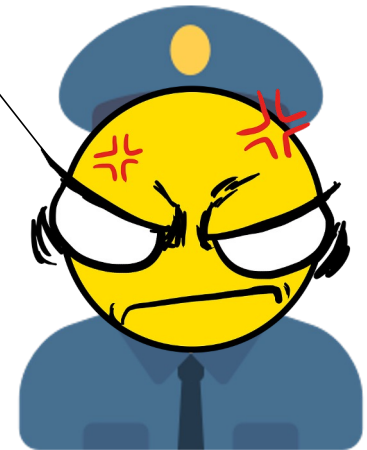


A



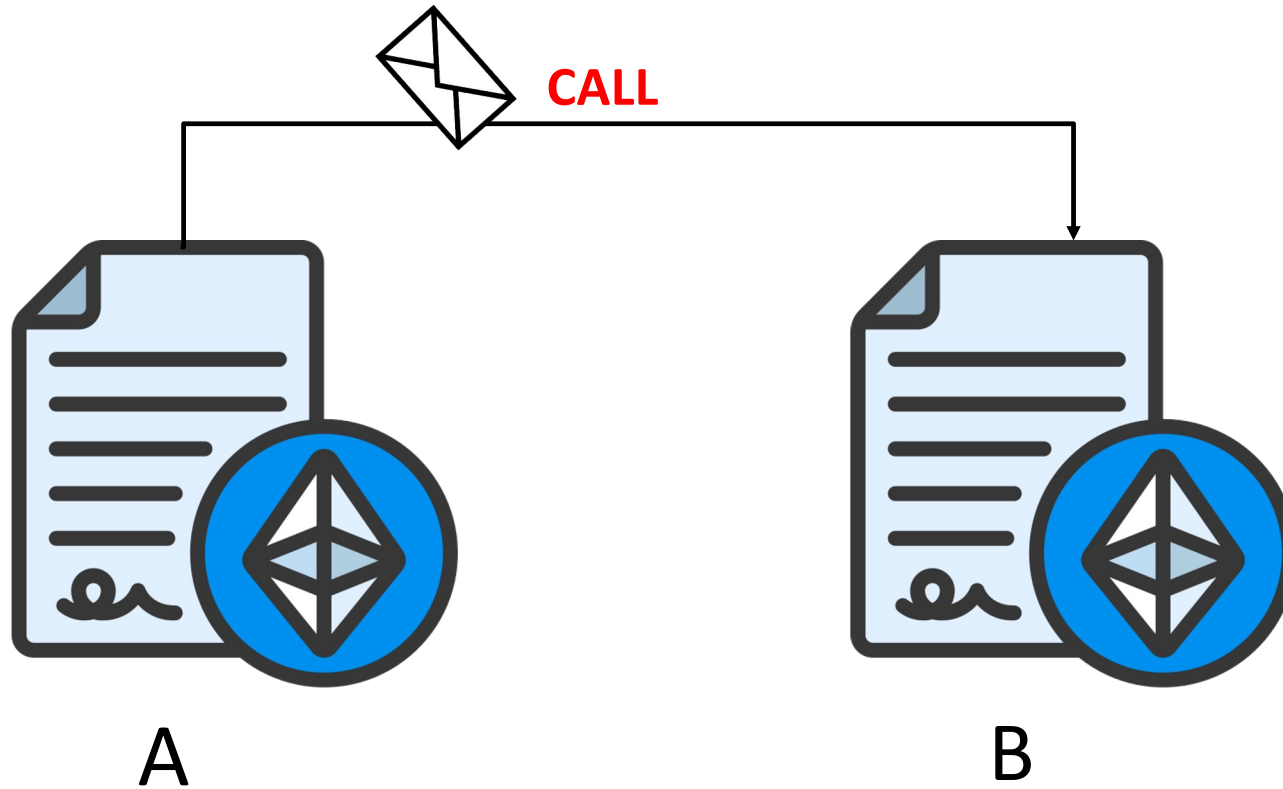
C  
Confused Deputy

But...  
I **trusted**  
you...

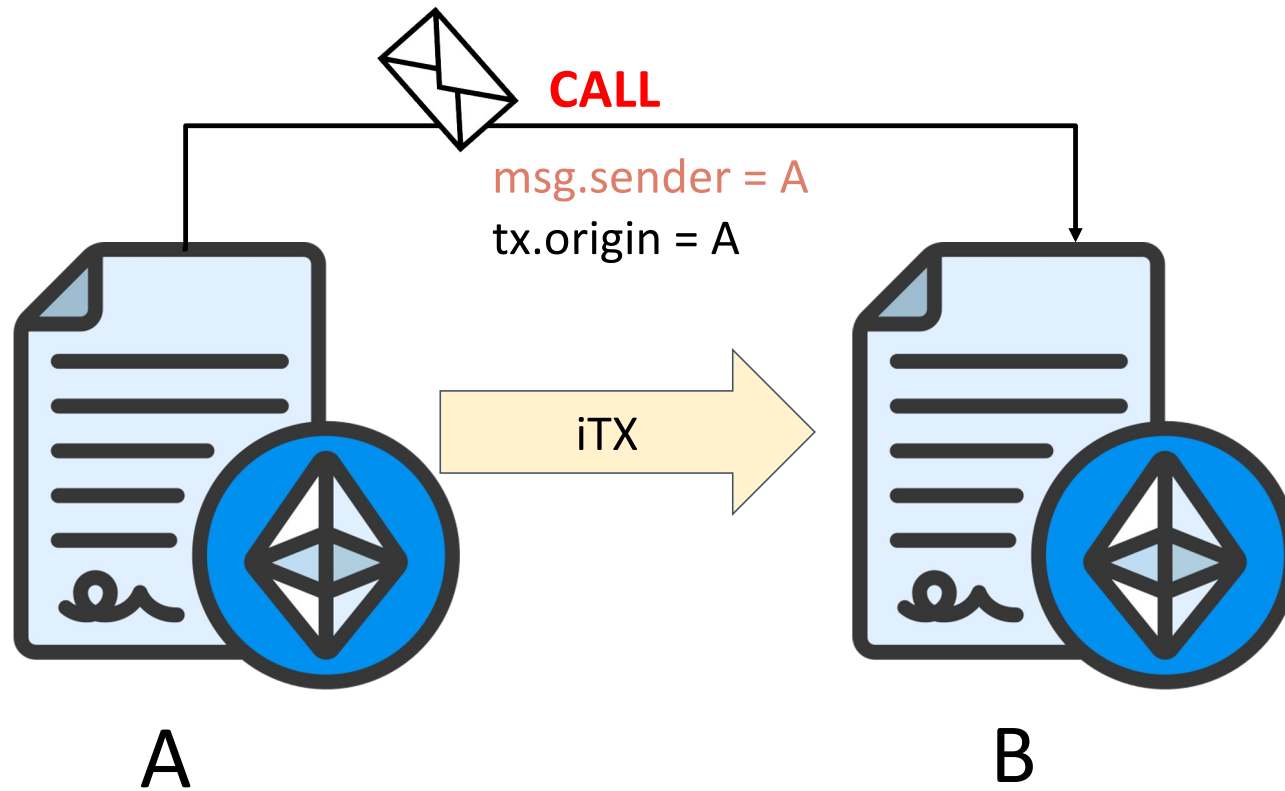


B  
Target

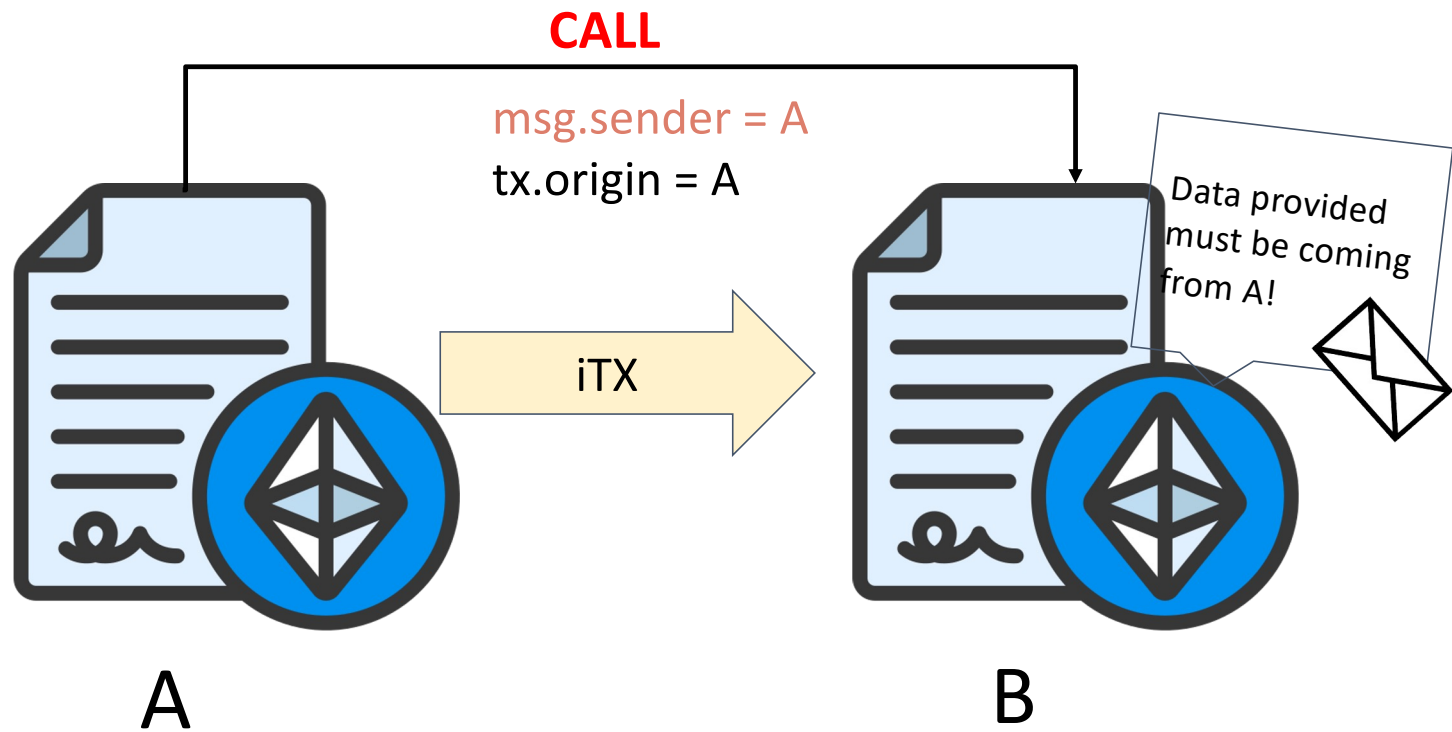
# Confused Contract



# Confused Contract



# Confused Contract

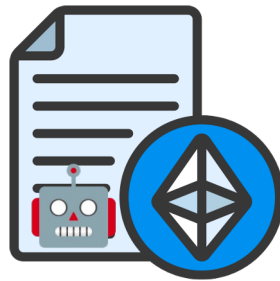




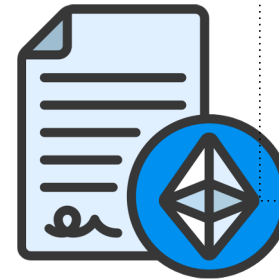
# Confused Contract



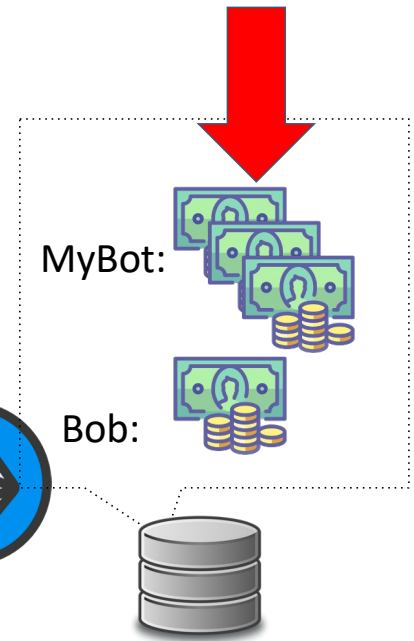
Alice



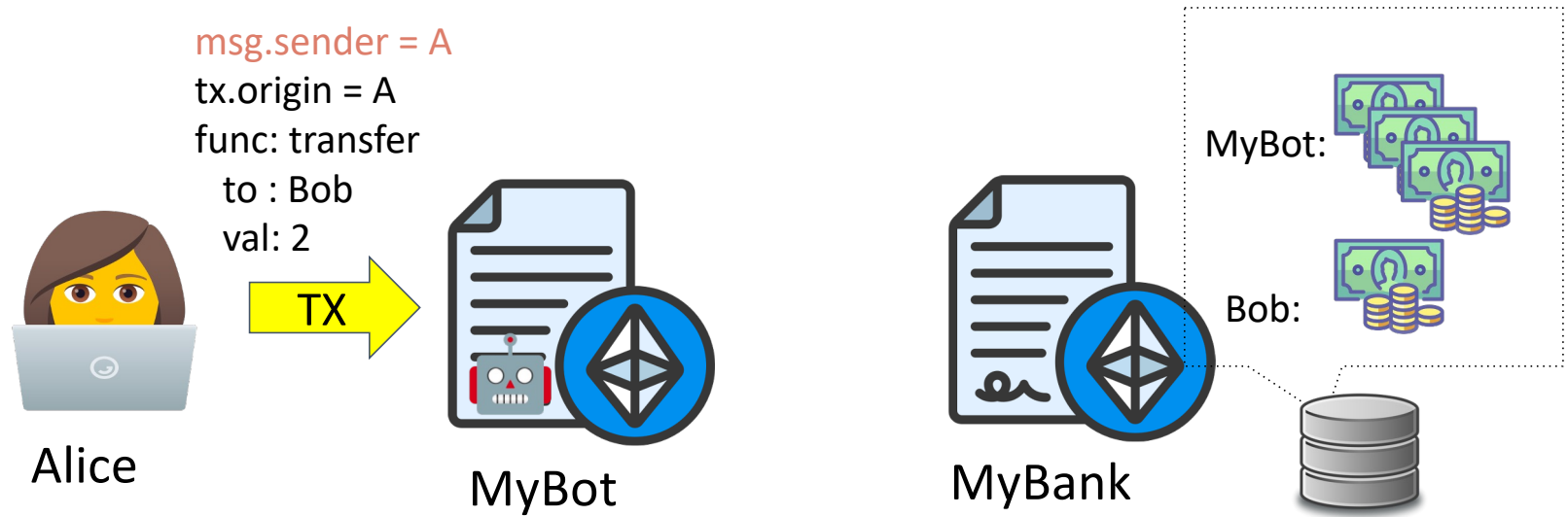
MyBot



MyBank

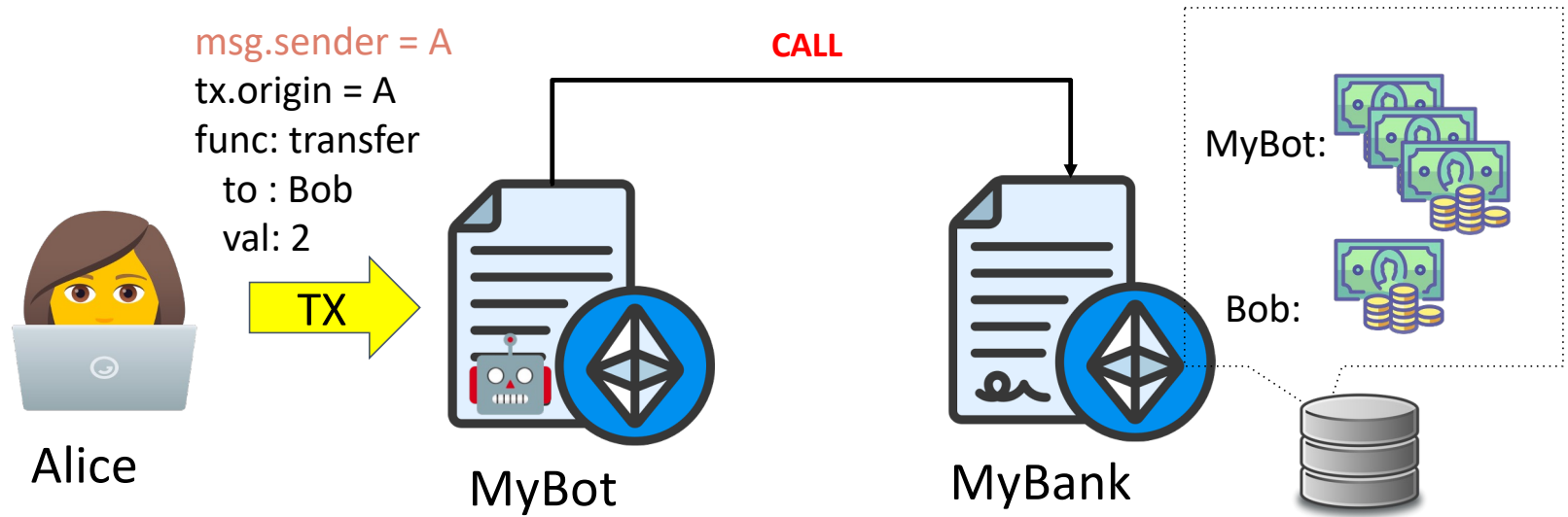


# Confused Contract



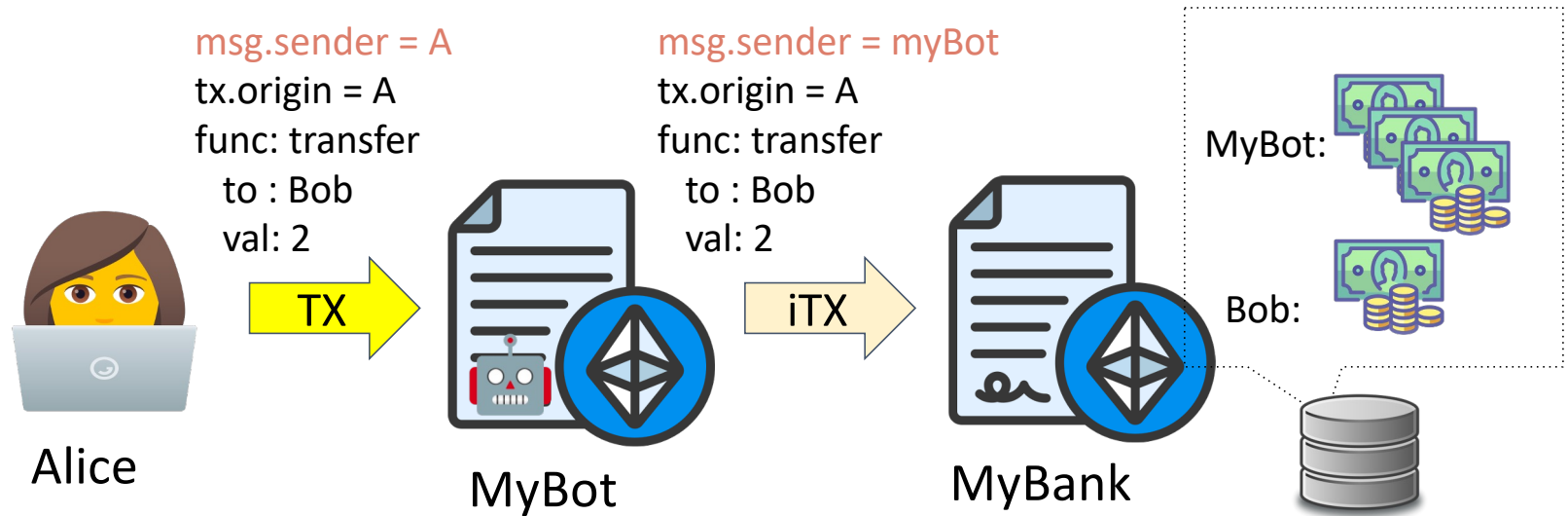
Transfer of funds  
(benign)

# Confused Contract



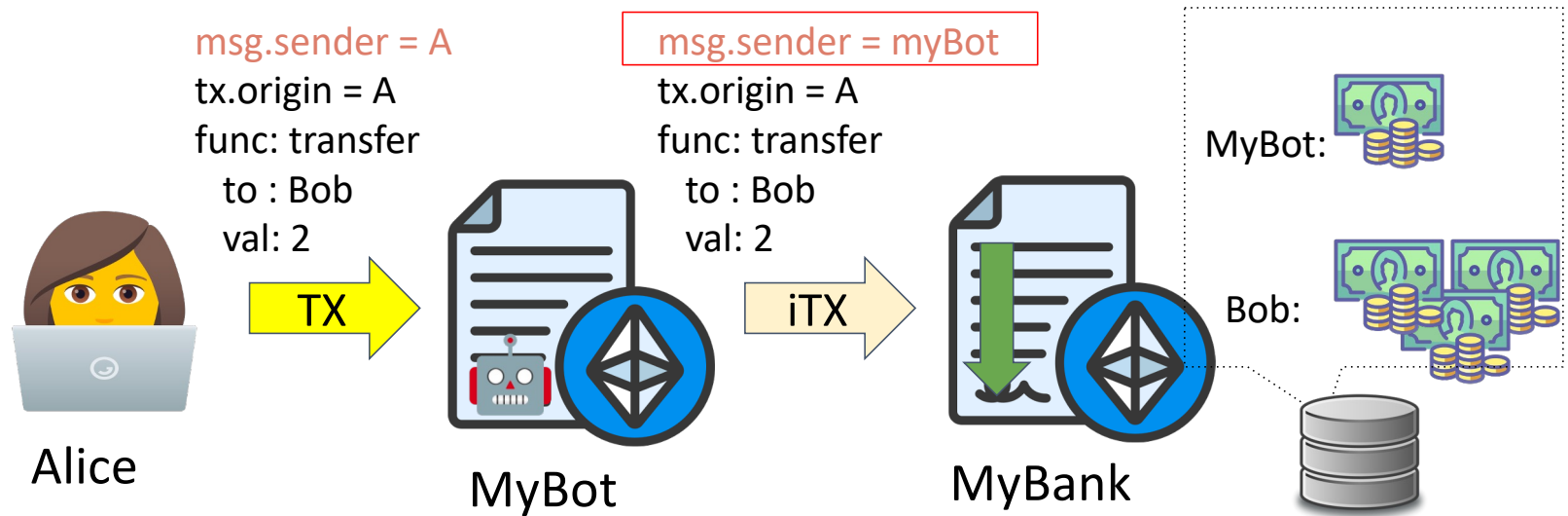
Transfer of funds  
(benign)

# Confused Contract



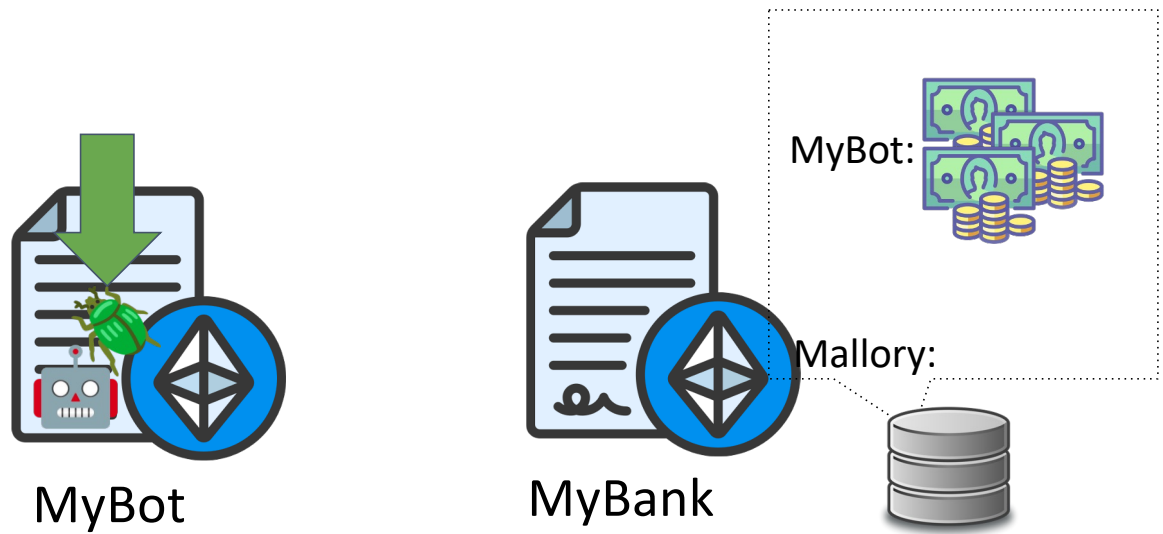
Transfer of funds  
(benign)

# Confused Contract



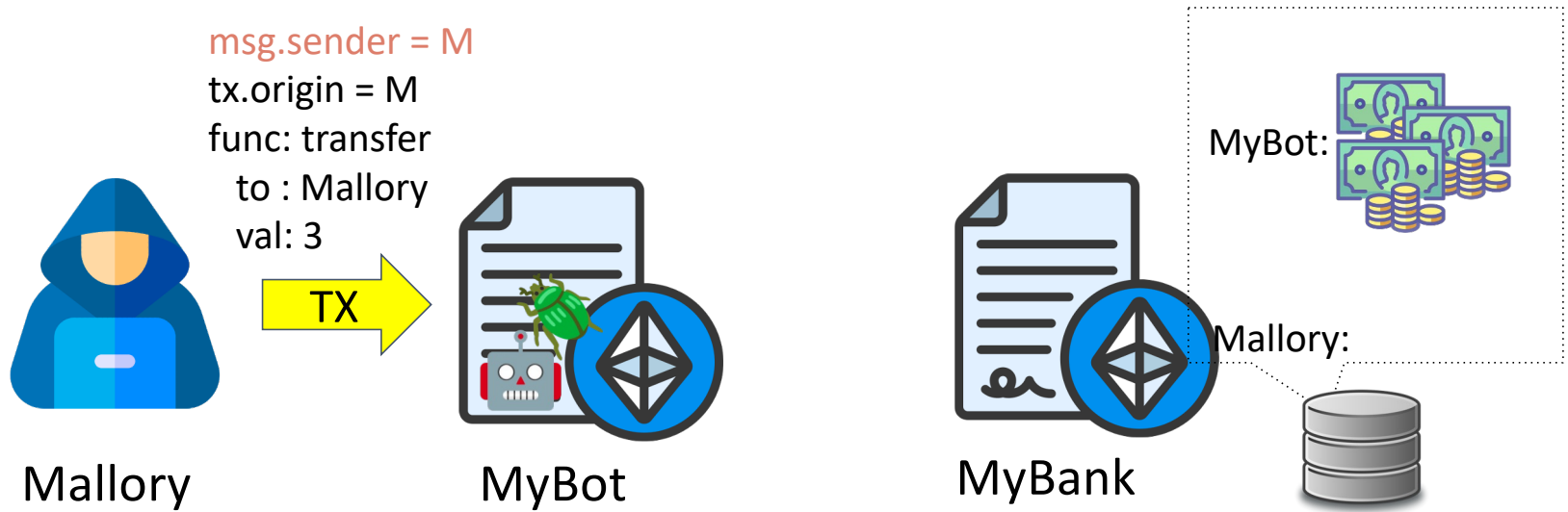
Transfer of funds  
(benign)

# Confused Contract



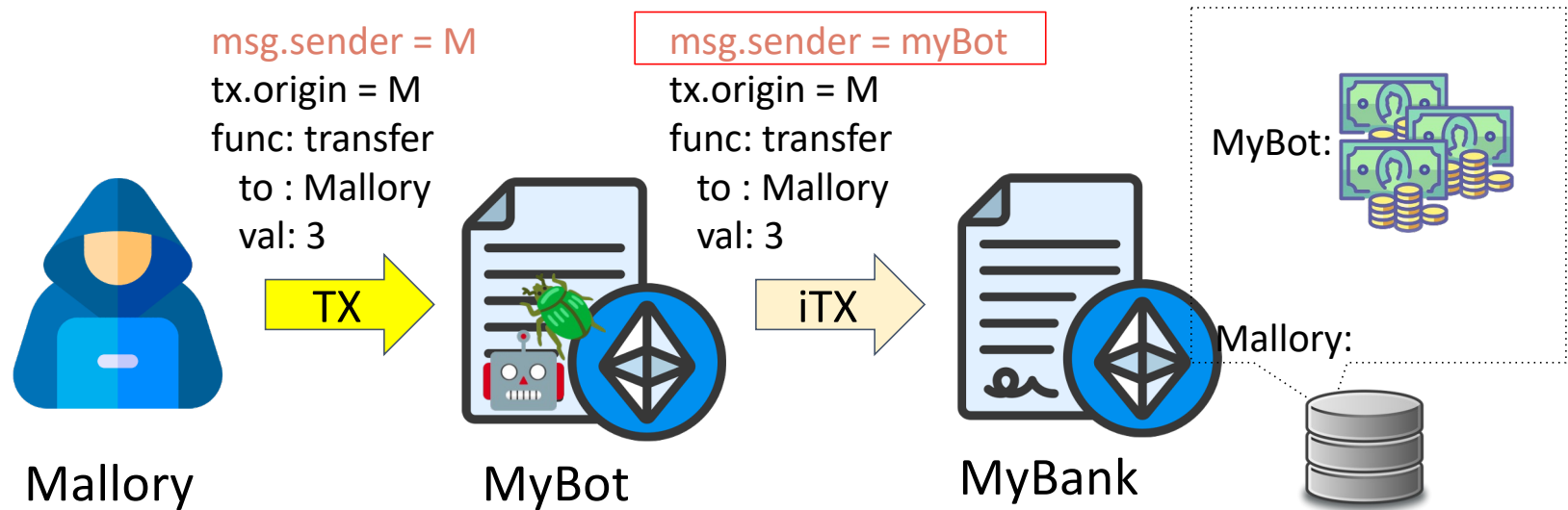
Transfer of funds  
(malicious)

# Confused Contract



Transfer of funds  
(malicious)

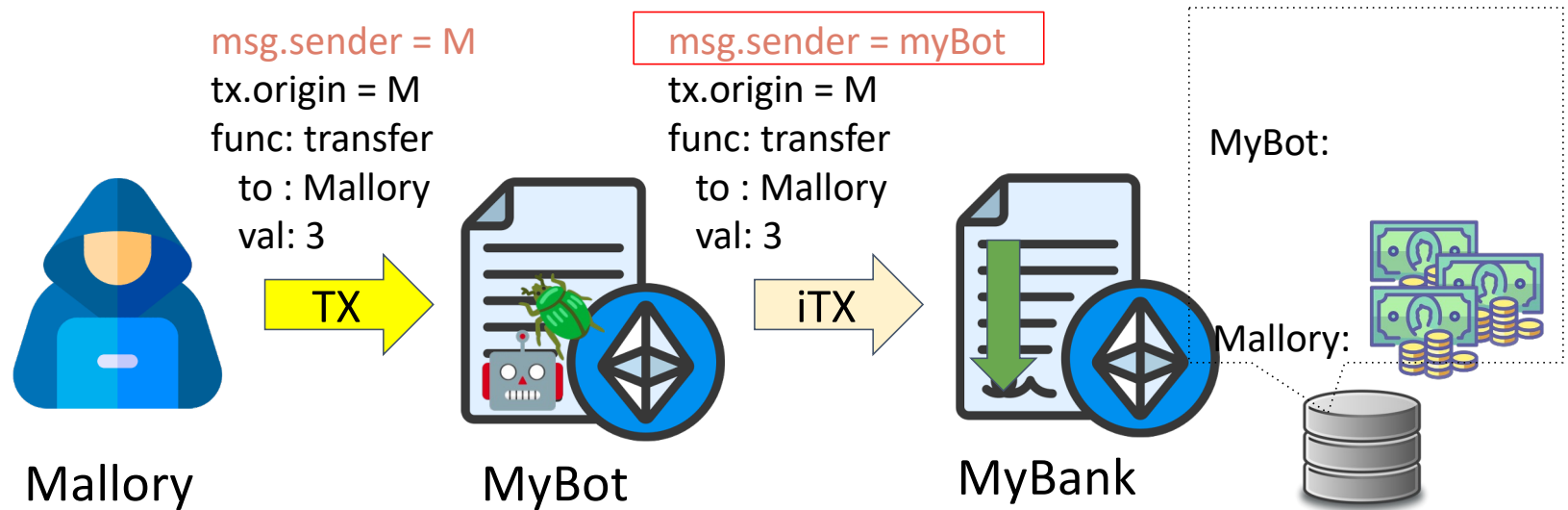
# Confused Contract



Transfer of funds  
(malicious)

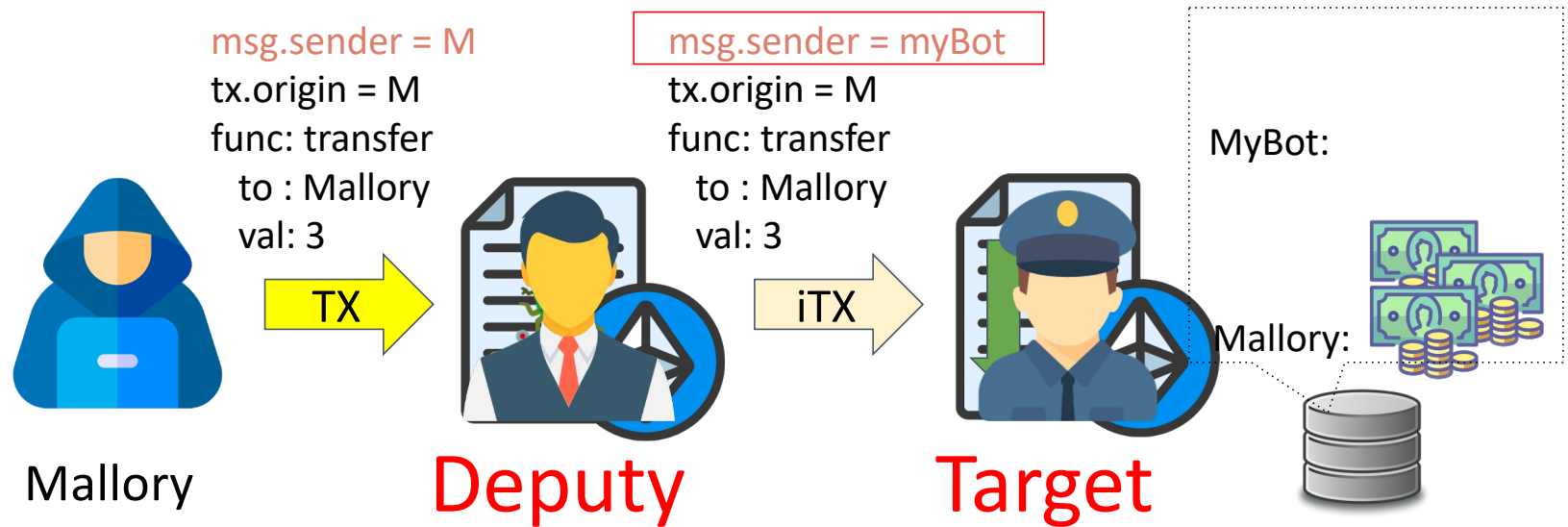


# Confused Contract



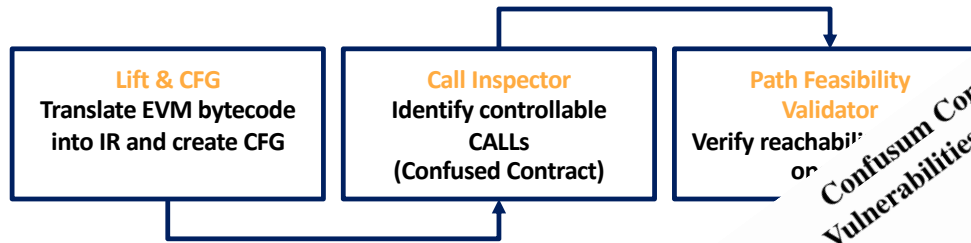
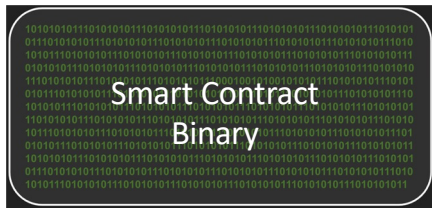
Transfer of funds  
(malicious)

# Confused Contract



Transfer of funds  
(malicious)

# KAI



**Confused Deputy Vulnerabilities in Ethereum Smart Contracts**

## Abstract

Smart contracts are immutable programs executed in the context of a globally distributed system known as a blockchain.

interest drove the market capitalization of Ethereum to over \$1 billion to 568 billion dollars in just one year.

- 2,000,000+ smart contracts
  - Deployed between December 2020 → Dec 2021
- 529 potential Confused Contracts
  - 84 warnings Confused Contract + Contract Target
- 13 working exploits for a total value of more than \$1,000,000

# Call To Action

- We need better tools to analyze smart contracts
  - Dynamic symbolic execution
  - Static analysis
  - Model checking
  - Fuzzing
  - Decompilers
- We need more people looking at smart contract
  - Start breaking stuff (responsibly) and collect amazing bug bounties!
- We need ways to recover stolen funds
  - Prevent money laundering
  - Reversible tokens (ERC-20R and ERC-721R proposal by Stanford researchers)

# Conclusions

- The DeFi ecosystem is a fascinating new target for security research
  - For both enthusiasts *and* detractors!
- Tools are primitive, human expertise is lacking
- If DeFi truly becomes the future of finance, we need to do something, or we are doomed...  
... and maybe it's a good thing!



# NFTs

- Of course, we didn't have the time to talk about NFTs...

## Understanding Security Issues in the NFT Ecosystem

Dipanjan Das

University of California, Santa Barbara  
Santa Barbara, California, USA  
dipanjan@cs.ucsb.edu

Priyanka Bose

University of California, Santa Barbara  
Santa Barbara, California, USA  
priyanka@cs.ucsb.edu

Nicola Ruardo

University of California, Santa Barbara  
Santa Barbara, California, USA  
ruaronicola@cs.ucsb.edu

Christopher Kruegel

University of California, Santa Barbara  
Santa Barbara, California, USA  
chris@cs.ucsb.edu

Giovanni Vigna

University of California, Santa Barbara  
Santa Barbara, California, USA  
vigna@cs.ucsb.edu

*ACM Conference on Computer and Communications Security (CCS), 2022*

# Thanks!

Questions to [vigna@ucsb.edu](mailto:vigna@ucsb.edu)

