



# Not Your Grandma's Smart Contract Verification



Florian  
Buenzli



Dana Drachsler-  
Cohen



Andrei  
Dan



Arthur  
Gervais



Quentin  
Hibon



Hubert  
Ritzdorf



Petar  
Tsankov



Martin  
Vechev

<http://blockchainsecurity.ethz.ch>

# Smart Contract *Security Bugs* in the News



Ethereum • News • Ethereum

The DAO, the distributed autonomous organization that had collected over \$150 million worth of ether, has reportedly been hacked, sparking a broad market sell-off.

A [leaderless organization](#) comprised of a series of smart contracts written on the Ethereum blockchain, the DAO has lost [3.6m ether](#), which is currently sitting in a separate wallet after being stolen by hackers.

## The DAO Falls Victim to Cyber Attack Leading Ethereum to Crash Over 20%

The event is still ongoing as hackers have already stolen over 3.5 million ETH from the DAO's coffers.

 [Avi Mizrahi](#) | Trading (Cryptocurrency) | Friday, 17/06/2016 | 12:45 GMT



Photo: Finance Magnates

[Share this article](#)    



## \$32 million worth of digital currency ether stolen by hackers

- Around 153,000 ether tokens worth \$32.6 million were taken by hackers on Wednesday.

## Hackers have stolen \$32 million in Ethereum in the second heist this week

Smart contract coding company Parity has issued a security alert, warning of a vulnerability in version 1.5 or later of its wallet software.

So far, 150,000 ethers, worth \$30 million (£23 million), have been reported by the company as stolen, data confirmed by [Etherscan.io](#).



[www.jamesedition.com](http://www.jamesedition.com)

Smart contract coding company Parity yesterday issued a security alert, warning of a vulnerability in version 1.5 or later of its wallet software. According to the company, so far 150,000 ethers have been stolen, worth nearly \$35 million at current price levels. The amount of the stolen ether has been confirmed by Etherscan.io.



# *Unprivileged* write to storage



Any user may  
change the  
wallet's owner



Wallet Contract

```
address owner = ...;  
  
function initWallet(address _owner) {  
    owner = _owner;  
}  
  
function withdraw(uint amount) {  
    if (msg.sender == owner) {  
        owner.transfer(amount);  
    }  
}
```

Only owner can  
send ether

An attacker used a similar bug to *steal \$30M* in July

# More Security Bugs...



Unexpected ether flows

# More Security Bugs...



Unexpected ether flows

---



Insecure coding, such as unprivileged writes (*e.g., Multisig Parity bug*)

# More Security Bugs...



Unexpected ether flows

---



Insecure coding, such as unprivileged writes (*e.g., Multisig Parity bug*)

---



Use of unsafe inputs (*e.g., reflection, hashing, ...*)

# More Security Bugs...



Unexpected ether flows

---



Insecure coding, such as unprivileged writes (*e.g., Multisig Parity bug*)

---



Use of unsafe inputs (*e.g., reflection, hashing, ...*)

---



Reentrant method calls (*e.g., DAO bug*)

# More Security Bugs...



Unexpected ether flows

---



Insecure coding, such as unprivileged writes (*e.g., Multisig Parity bug*)

---



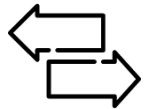
Use of unsafe inputs (*e.g., reflection, hashing, ...*)

---



Reentrant method calls (*e.g., DAO bug*)

---



Manipulating ether flows via transaction reordering



# Transaction *reordering*



The owner can  
change the price



## Token Contract

```
uint price = 10;  
address owner;  
  
function setPrice(uint newPrice) {  
    if (msg.sender == owner)  
        price = newPrice;  
}  
  
function sellToken() {  
    msg.sender.transfer(price);  
}
```

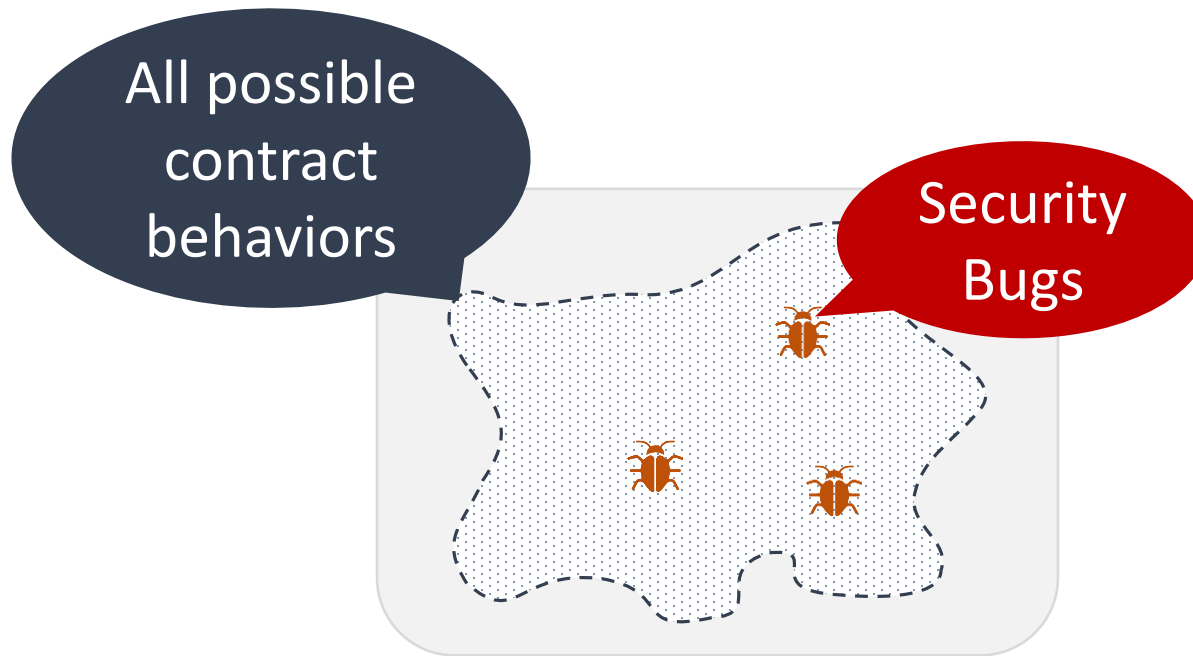
A user can buy with  
the current price

The two operations do not commute

The background of the slide features a dark blue, textured surface with a pattern of diagonal lines. Overlaid on this are various mechanical and digital motifs. Several gears of different sizes are scattered across the frame, some in shades of teal and others in a lighter blue. A network of thin, light blue lines connects various points, resembling a circuit board or a data flow diagram. Small circles and dots are also visible, some acting as nodes in the network. The overall aesthetic is high-tech and industrial.

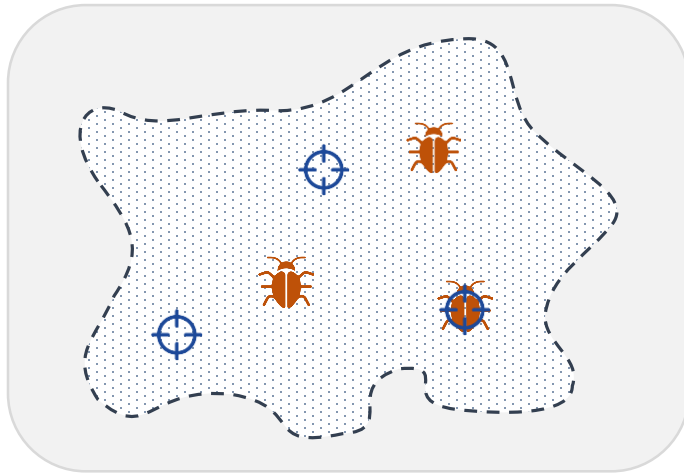
# Automated Security Analysis

# Automated Security Analysis Approaches



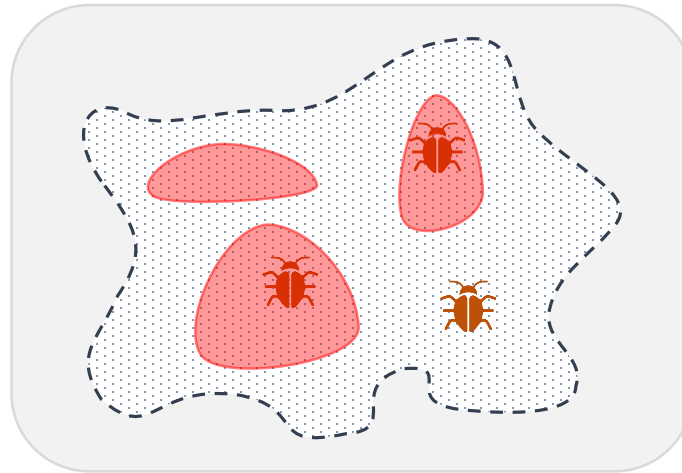
**Problem:** Cannot enumerate all possible contract behaviors...

# Security Analysis Approaches



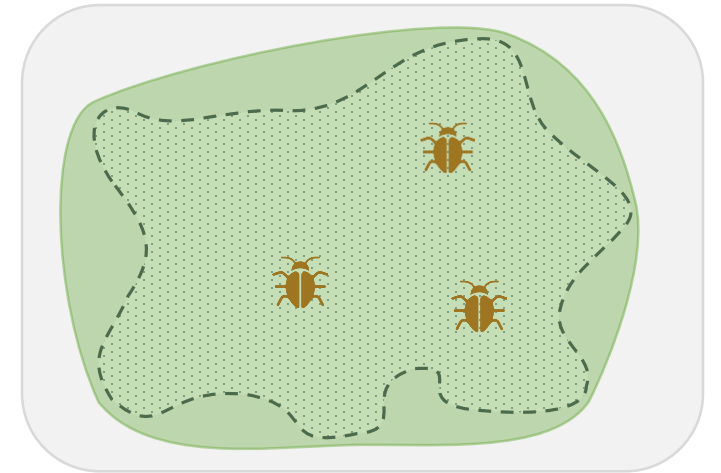
Testing

Report true bugs  
Can miss bugs



Dynamic (symbolic) analysis

Report true bugs  
Can miss bugs



Automated verification

Can report false alarms  
No missed bugs

The background is a dark blue gradient with a subtle diagonal line pattern. It is overlaid with a complex network of light blue and white geometric shapes. These include various sizes of gears, interconnected nodes, and lines that resemble a circuit board or a data network. Some elements are semi-transparent, creating a layered effect. The overall aesthetic is technical and futuristic.

# Current State of Automated Analysis for Ethereum Smart Contracts

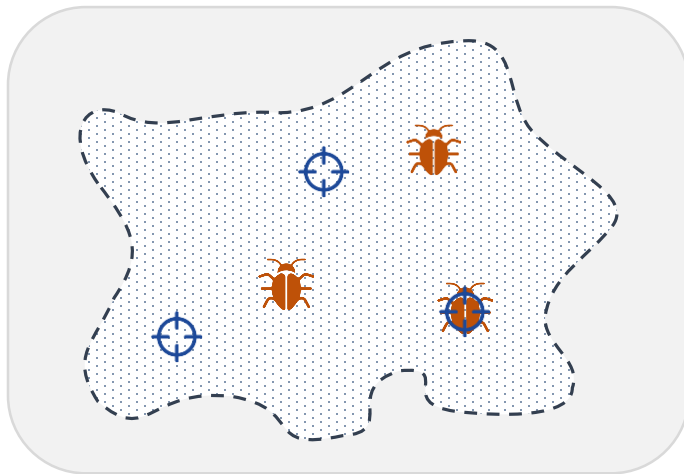


# Security Analysis Approaches



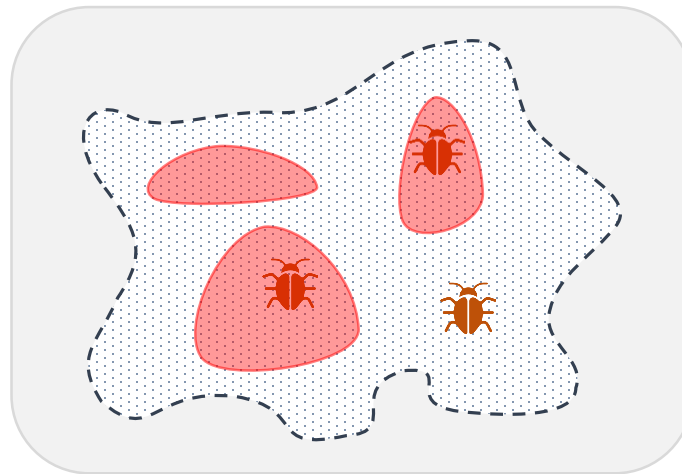
Populus

Oyente



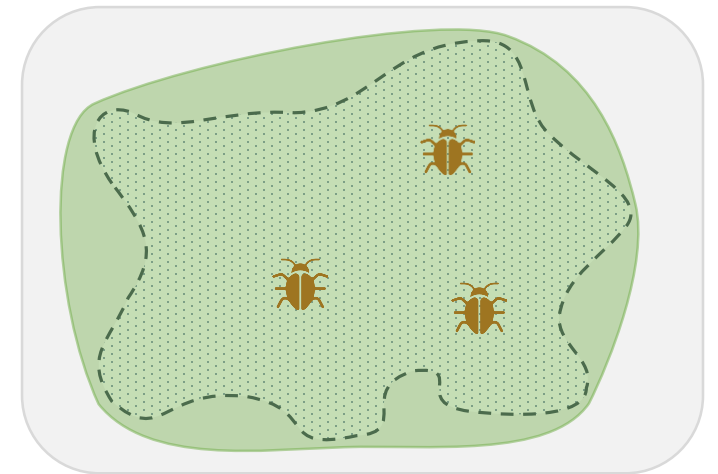
Testing

Report true bugs  
Can miss bugs



Dynamic (symbolic) analysis

Report true bugs  
Can miss bugs



Automated verification

Can report false alarms  
No missed bugs



[www.securify.ch](http://www.securify.ch)

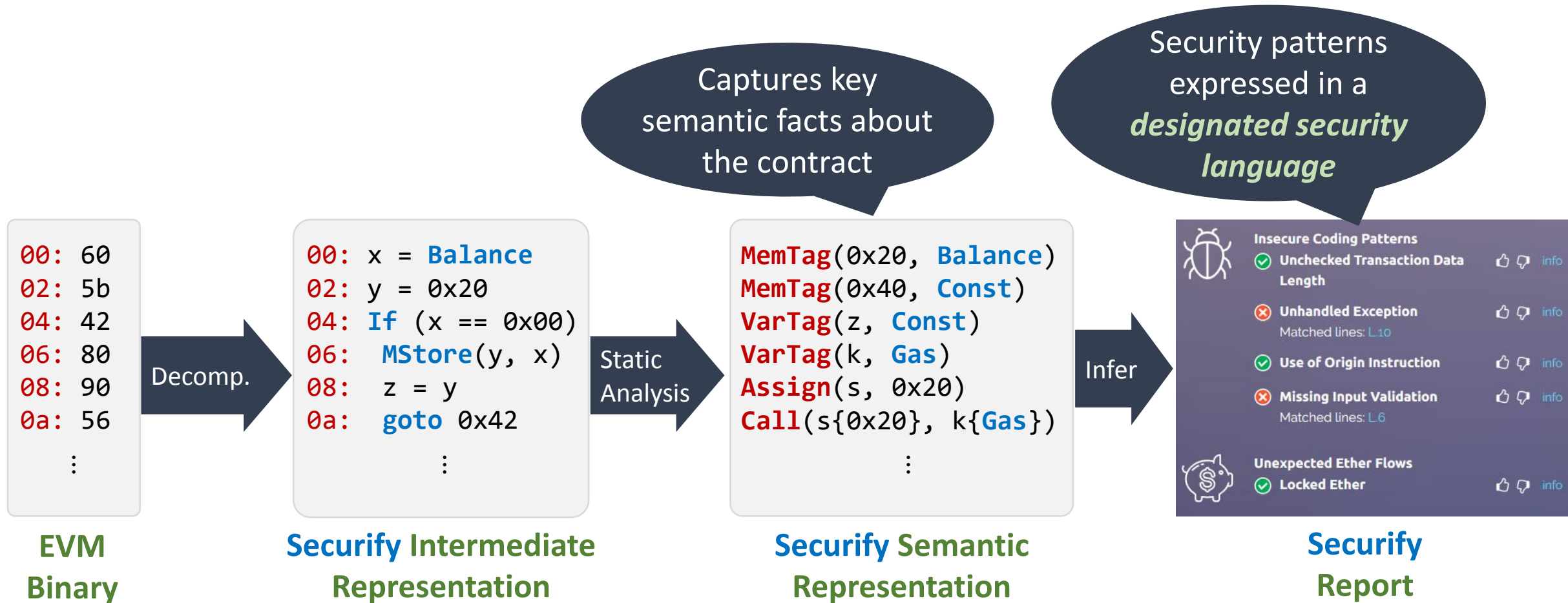
Fully *automated*, one-click,  
*formal verification* system for  
Ethereum smart contracts

The background is a dark blue field with a fine, diagonal hatched pattern. Overlaid on this are various light blue and white geometric elements: several interlocking gears of different sizes, some with solid centers and others as outlines; a network of thin lines connecting small circles and hexagons, resembling a circuit board or a data flow diagram; and various small symbols like arrows and dots. A semi-transparent horizontal band runs across the middle of the image, and the word "Demo" is centered within it.

**Demo**



# Securify: Under the Hood



Fully automated, easily extensible

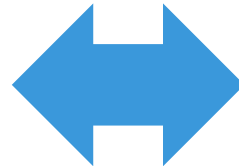
# ChainSecurity



Swiss-based startup that provides intelligent security solutions for *blockchains* and *smart contracts*



*Automated*  
Security Analysis  
Systems



Comprehensive  
Smart Contract  
Auditing

<https://chainsecurity.com>

# Summary

## Research



Fully automated



Strong guarantees



Extensible



<https://www.securify.ch>

## Product

Get in touch with our team  
of **security** / **blockchain** /  
**program analysis** experts



<https://chainsecurity.com>



[contact@chainsecurity.com](mailto:contact@chainsecurity.com)



[@chain\\_security](https://twitter.com/chain_security)