29.01.2024

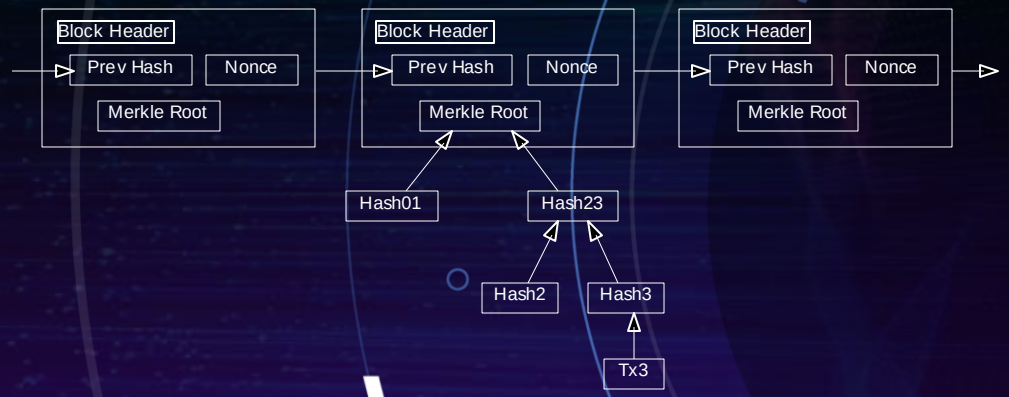
Smart contract audit
Blockchain security

Steve Huguenin

What is blockchain?

Nakamoto, Satoshi (31 October 2008). "Bitcoin: A Peer-to-Peer Electronic Cash System“ https://bitcoin.org/bitcoin.pdf*

*The term blockchain is not found in this article, but the fundamentals behind Proof-of-work chain remain those of blockchain.



Smart contracts (1/2)

Abstract

*Smart contracts combine **protocols** with user interfaces to **formalize and secure relationships over computer networks**. Objectives and principles for the design of these systems are derived from **legal principles, economic theory, and theories of reliable and secure protocols**. Similarities and differences between smart contracts and traditional business procedures based on written contracts, controls, and static forms are discussed. By using cryptographic and other security mechanisms, we can secure many algorithmically specifiable relationships from breach by principals, and from eavesdropping or malicious interference by third parties, up to considerations of time, user interface, and completeness of the algorithmic specification. This article discusses protocols with application in important **contracting areas**, including **credit**, **content rights management**, **payment systems**, and **contracts with bearer**.*

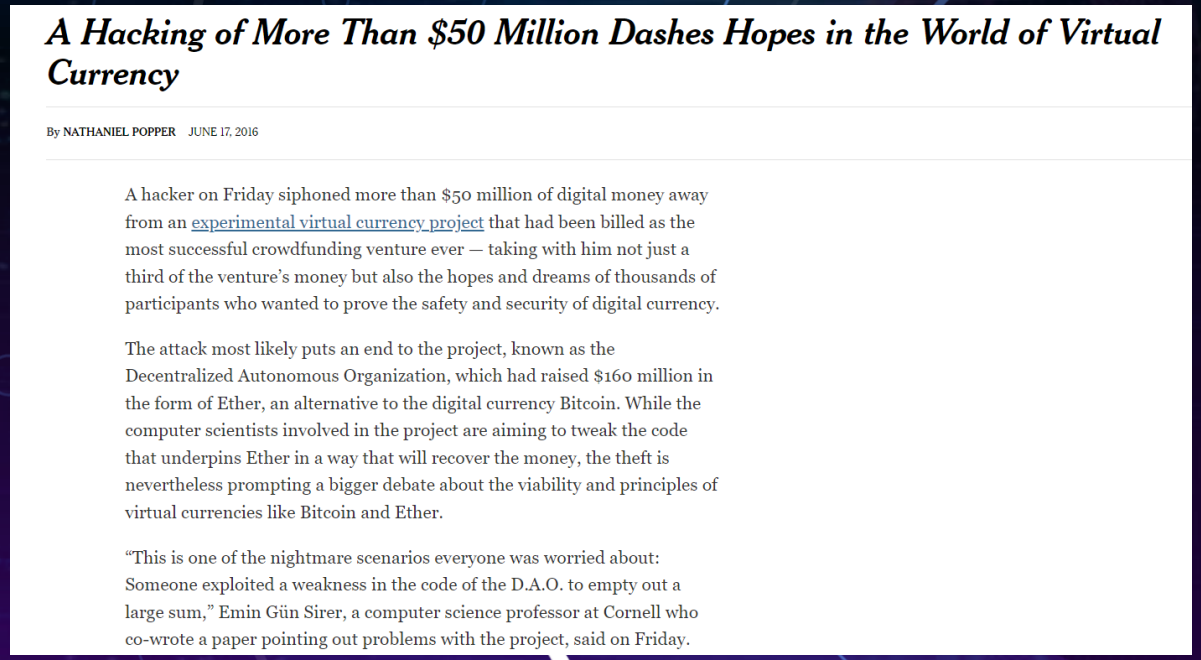
Szabo, N. 1997. Formalizing and Securing Relationships on Public Networks. *First Monday*. 2, 9 (Sep. 1997). DOI:https://doi.org/10.5210/fm.v2i9.548.

Smart contracts (2/2)

- Smart contracts are developed to execute critical functions of a complex system with real-life applications.
- Any error found in a smart contract can represent damage for the user experience and the entire world economy.
- Tactics have been developed to assure the safety of smart contracts after their development on blockchain.

TheDAO Hack

Popper, Nathaniel (17 June 2016). "Hacker May Have Taken $50 Million From Cybercurrency Project". The New York Times. Archived from the original on 20 June 2017. Retrieved 3 March 2017.



A Hacking of More Than $50 Million Dashes Hopes in the World of Virtual Currency

By NATHANIEL POPPER JUNE 17, 2016

A hacker on Friday siphoned more than $50 million of digital money away from an experimental virtual currency project that had been billed as the most successful crowdfunding venture ever — taking with him not just a third of the venture's money but also the hopes and dreams of thousands of participants who wanted to prove the safety and security of digital currency.

The attack most likely puts an end to the project, known as the Decentralized Autonomous Organization, which had raised $160 million in the form of Ether, an alternative to the digital currency Bitcoin. While the computer scientists involved in the project are aiming to tweak the code that underpins Ether in a way that will recover the money, the theft is nevertheless prompting a bigger debate about the viability and principles of virtual currencies like Bitcoin and Ether.

"This is one of the nightmare scenarios everyone was worried about: Someone exploited a weakness in the code of the D.A.O. to empty out a large sum," Emin Gün Sirer, a computer science professor at Cornell who co-wrote a paper pointing out problems with the project, said on Friday.

Celsius Network Crash With Bankruptcy

Yaffe-Bellany, David (June 13, 2022). "Celsius Network Leads Crypto Markets into Another Free Fall". The New York Times. ISSN 0362-4331. Archived from the original on June 14, 2022. Retrieved June 14, 2022.

Gladstone, Alexander; Ge Huang, Vicky; Biswas, Soma (July 14, 2022). "Crypto Crash Drags Lender Celsius Network Into Bankruptcy". Wall Street Journal. Retrieved July 14, 2022.

BANKRUPTCY

Crypto Crash Drags Lender Celsius Network Into Bankruptcy

The crypto lending platform's business model became untenable as digital currency prices collapsed

By Alexander Gladstone, Vicky Ge Huang and Soma Biswas

Updated July 13, 2022 9:51 pm ET | WSJ PRO

Share Resize 72 Listen (2 min)

When cryptocurrency lending platform Celsius froze user accounts amid a plunge in valuations, it sent ripples across the industry and raised questions about what happens to user assets if a crypto platform files for bankruptcy. WSJ's Vicky Ge Huang explains. Photo illustration: Jordan Kranse

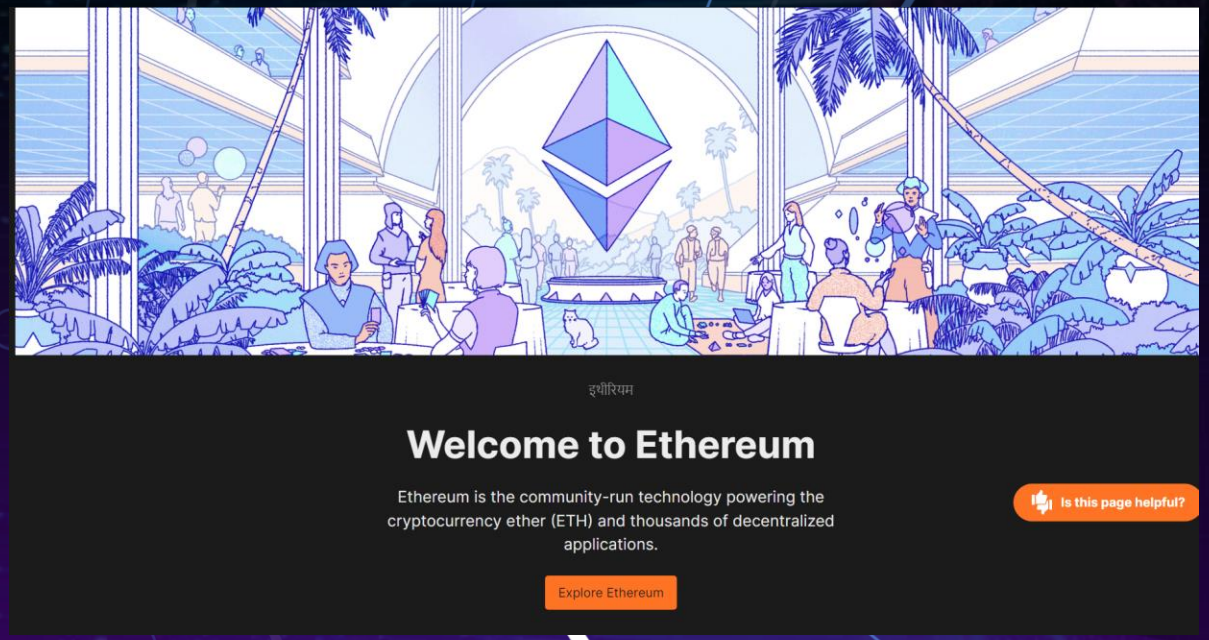
Cryptocurrency lender Celsius Network LLC filed for bankruptcy protection Wednesday, a month after halting withdrawals in the wake of a collapse in digital currency prices that stretched the platform's business model past the breaking point.

The chapter 11 filing in New York follows weeks of market speculation about Celsius, which built itself into one of the biggest cryptocurrency lenders on a pitch that it was less risky than a bank, and with better returns for its customers. But it overextended itself offering lofty yields to crypto depositors and making

Ethereum

Ethereum is a network of computers all over the world that follow a set of rules called the Ethereum protocol. The Ethereum network acts as the foundation for communities, applications, organizations and digital assets that anyone can build and use. […]

https://ethereum.org/what-is-ethereum



Solidity

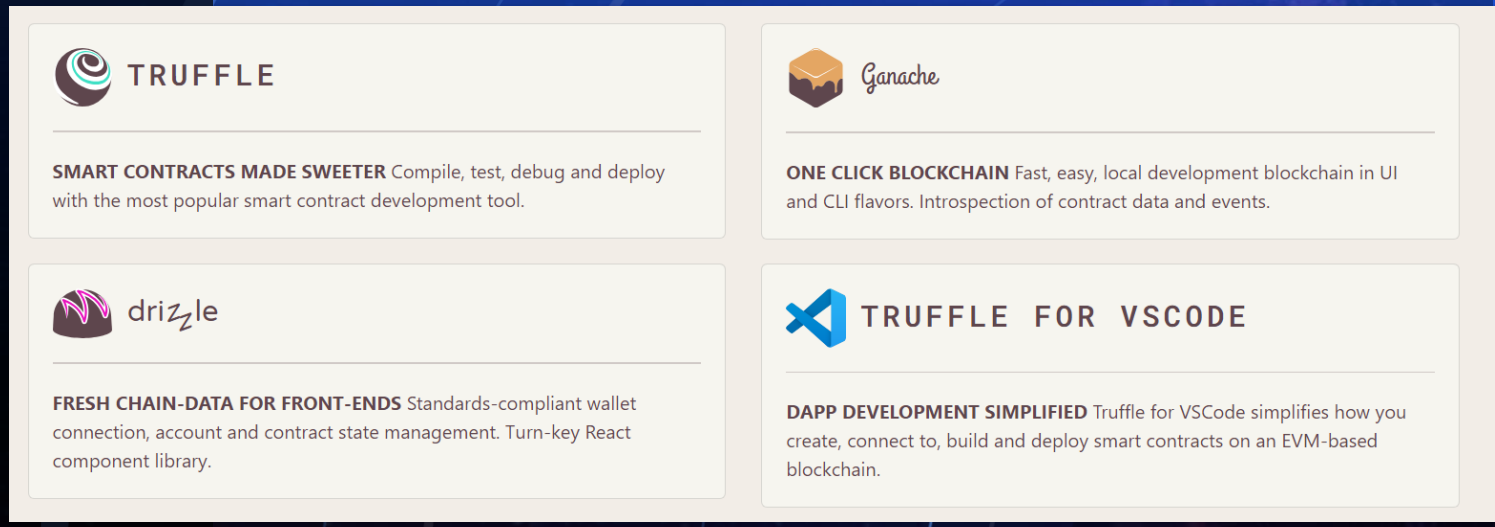
A statically-typed curly-braces programming language designed for developing smart contracts that run on Ethereum.

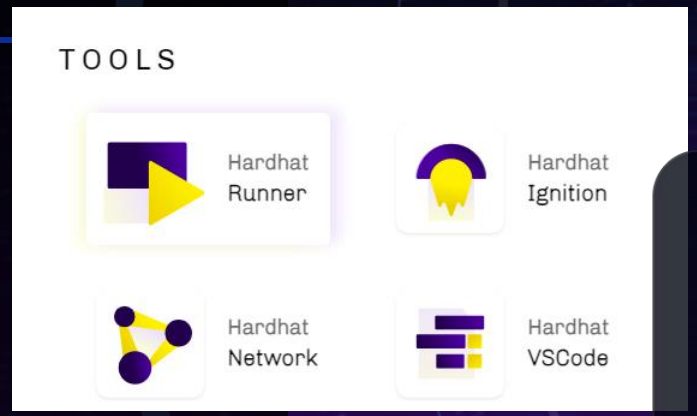
```solidity
pragma solidity 0.8.7;

contract VendingMachine {

    // Declare state variables of the contract
    address public owner;
    mapping (address => uint) public cupcakeBalances;

    // When 'VendingMachine' contract is deployed:
    // 1. set the deploying address as the owner of the contract
    // 2. set the deployed smart contract's cupcake balance to 100
    constructor() {
        owner = msg.sender;
        cupcakeBalances[address(this)] = 100;
    }

    // Allow the owner to increase the smart contract's cupcake balance
    function refill(uint amount) public {
        require(msg.sender == owner, "Only the owner can refill.");
        cupcakeBalances[address(this)] += amount;
    }

    // Allow anyone to purchase cupcakes
    function purchase(uint amount) public payable {
        require(msg.value >= amount * 1 ether, "You must pay at least 1 ETH per cupcake");
        require(cupcakeBalances[address(this)] >= amount, "Not enough cupcakes in stock to complete this purchase");
        cupcakeBalances[address(this)] -= amount;
        cupcakeBalances[msg.sender] += amount;
    }
}

```

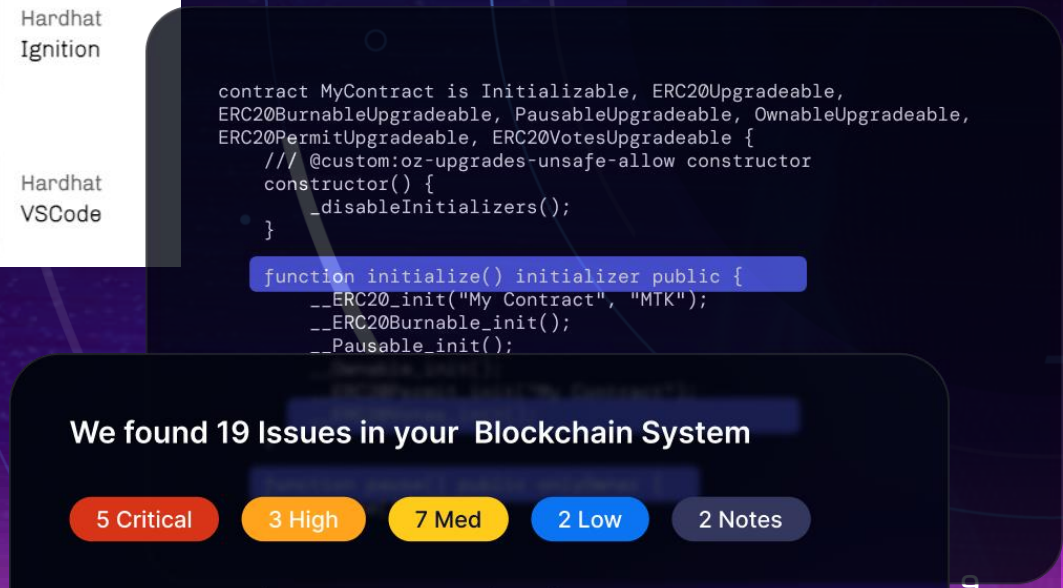
Tooling

Solc-verify is particulary handy

Hajdu, Á., Jovanović, D. (2020). SOLC-VERIFY: A Modular Verifier for Solidity Smart Contracts. In: Chakraborty, S., Navas, J. (eds) Verified Software. Theories, Tools, and Experiments. VSTTE 2019. Lecture Notes in Computer Science(), vol 12031. Springer, Cham. https://doi.org/10.1007/978-3-030-41600-3_11







Business cases

Let’s discuss some of the best open-access audit reports

Thank you

Steve Huguenin

University of Luxembourg FTSM Incoming

steve.huguenin.001@student.uni.lu