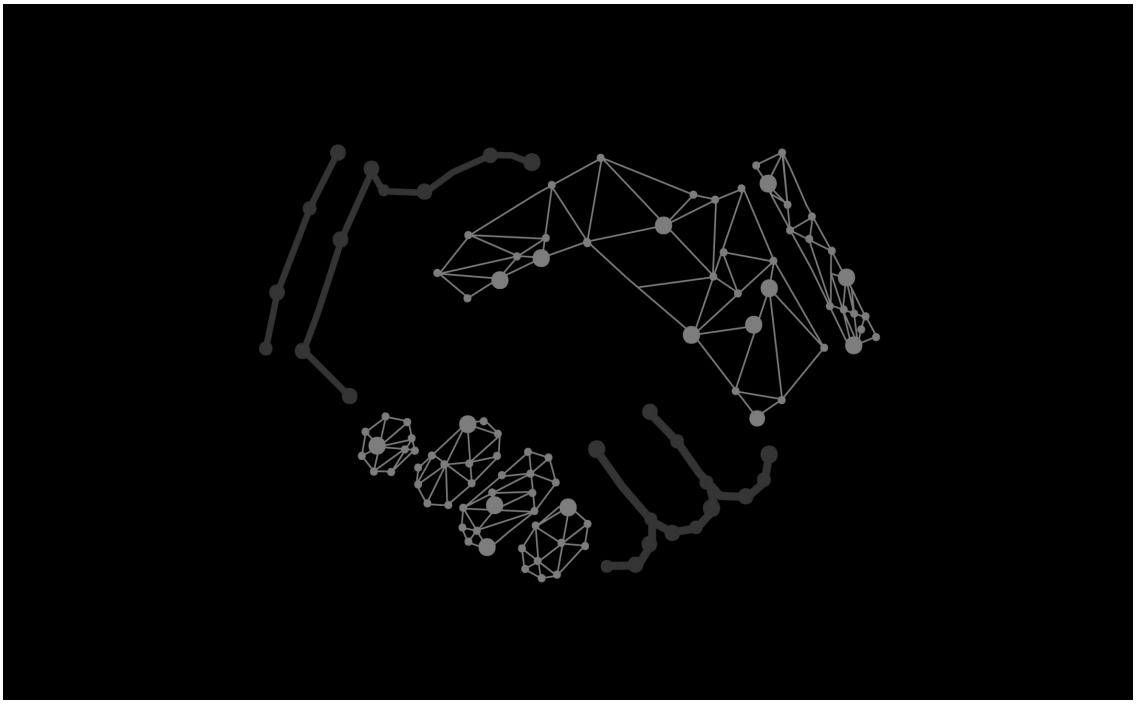


LYNNE CARTY

Connectivity

Ethereum’s smart contracts are full of holes

Blockchain-powered computer programs promise to revolutionize the digital economy, but new research suggests they’re far from secure.

by Mike Orcutt March 1, 2018

Computer programs that run on blockchains are shaking up the financial system. But much of the hype around what are called smart contracts is just that. It’s a brand-new field. Technologists are just beginning to figure out how to design them so they can be relied on

not to lose people's money, and—as a new survey of Ethereum smart contracts illustrates—security researchers are only now coming to terms with what a smart-contract vulnerability even looks like.

This piece appears in our twice-weekly newsletter Chain Letter, which covers the world of blockchain and cryptocurrencies. Sign up here—it's free!

Digital vending machines: The term "smart contract" comes from digital currency pioneer Nick Szabo, who coined it more than 20 years ago (and who may or may not be Satoshi Nakamoto). The basic idea, he wrote, is that "many kinds of contractual clauses (such as collateral, bonding, delineation of property rights, etc.) can be embedded in the hardware and software we deal with, in such a way as to make a breach of contract expensive (if desired, sometimes prohibitively so) for the breacher." Szabo called physical vending machines a "primitive ancestor of smart contracts," since they take coins and dispense a product and the correct change according to the displayed price.

Enter the blockchain: Today, the most common conception of a smart contract is a computer program stored on a blockchain. A blockchain is essentially a shared accounting ledger that uses cryptography and a network of computers to track assets and secure the ledger from tampering. For Bitcoin, that gives two parties who don't know each other an ironclad guarantee that an agreed upon transfer of funds will happen as expected—that is, no one will get cheated.

Smart contracts are where things get interesting. Using a smart contract, two people could create a system that withdraws funds from one person's account—a parent's, let's say—and deposits them

into a child's account if and when the child's balance falls below a certain level. And that's just the simplest example—in theory, smart contracts can be used to program all kinds of financial agreements, from derivatives contracts to auctions to blockchain-powered escrow accounts.

ICOs everywhere: One of the most popular applications of smart contracts has been to create new cryptocurrencies. A few of them have provided glimpses of a new kind of economy in which a purpose-made digital currency can be used for a "decentralized" service, like data storage or digital currency trading. Investor excitement over the promise of such applications has helped fuel the ICO craze, which has raised over $5 billion. (What the hell is an ICO? ← Here's a primer)

But hold your horses: Technologists still don't have a full picture of what a security hole in a smart contract looks like, says Ilya Sergey, a computer scientist at University College London, who coauthored a study on the topic published last week.

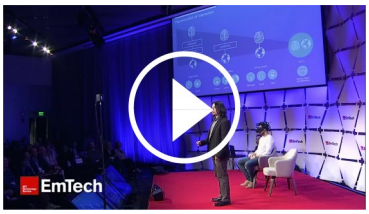
Users learned this the hard way in 2016 when a hacker stole $50 million from the so-called Decentralized Autonomous Organization, which was based on the Ethereum blockchain. And in November around $150 million suddenly became inaccessible to users of the wallet service Parity, which is also rooted in Ethereum.

Sergey and colleagues used a novel tool to analyze a sample of nearly one million Ethereum smart contracts, flagging around 34,000 as vulnerable—including the one that led to the Parity mishap. Sergey compares the team's work to interacting with a vending machine, as though the researchers randomly pushed buttons and recorded the conditions that made the machine act in unintended ways. "I believe

that a large number of vulnerabilities are still to be discovered and formally specified,” Sergey says.

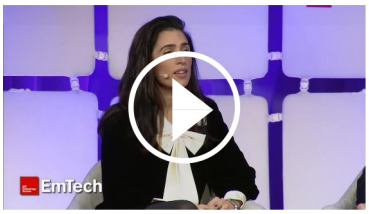
Related Video

More videos



Connectivity

Technology Spotlight: Mind-controlled VR 24:21



Connectivity

Yasmin Green: Using Technology to Make the World a Better Place 04:04

Connectivity

What is social media doing to society? 25:45

More from Connectivity

What it means to be constantly connected with each other and vast sources of information.

01

US conservatives spread tweets by Russian trolls over 30 times more often than liberals

The first detailed analysis of how misinformation spread through the Twittersphere during the 2016 election also shows that the most retweets of troll content came from Tennessee and Texas.

by Emerging Technology from the arXiv

02

The Travel Ecosystem: An Industry on the Go

Amadeus, a behind-the-scenes technology provider serving the entire travel ecosystem, has transformed its technology backbone to enable the new personalized and seamless digital experiences consumers crave.

by MIT Technology Review Insights