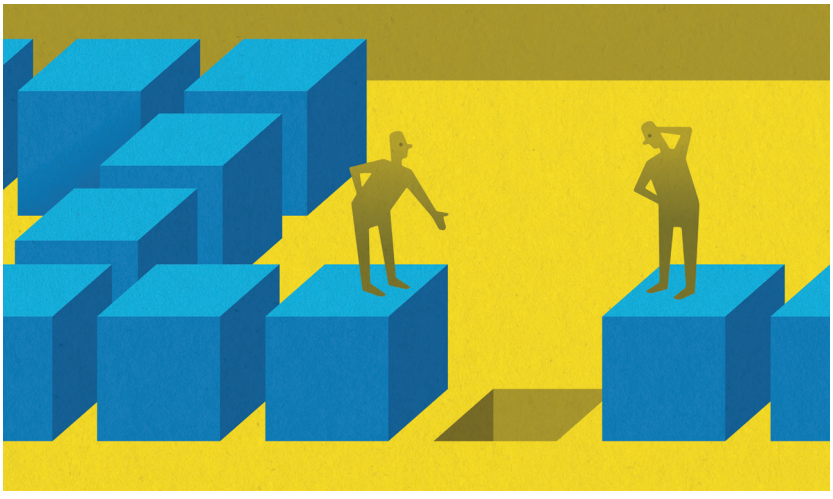
ONLY HUMAN

Blockchain's flaws are being discovered the hard way, says Brunswick's **CARLTON WILKINSON.**

THE TITANIC WAS "UNSINKABLE"—UNTIL IT sank. Now, blockchain, long touted as "unhackable," has been hacked. But while the Titanic sank only once, blockchain is destined to hit its iceberg over and over again.

Blockchain is widely seen as a potential foundation for all transactions—money, medical records, personal identities, elections, you name it. Brunswick Review first noted the technology's potential in 2016 when, as the vehicle of pioneer cryptocurrency Bitcoin, it was only beginning to spark. Today, it has exploded.

"Blockchain developer" was No. 1 on LinkedIn's list of emerging careers in 2018, topping new high-growth job titles such as "Machine Learning Engineer" and "Application Sales Executive." In addition to startups, interested companies include stalwarts like IBM, Fidelity Investments and Intercontinental Exchange, owners of the New York Stock Exchange.



Social media giants such as Facebook have hinted that they're working on their own blockchain-based cryptocurrencies. Even central banks are reported to be looking into the technology. Soon, many common transactions could be linked to a blockchain.

All that makes any vulnerability worrisome. Since the start of 2017, a total of nearly $2 billion worth of cryptocurrency has been publicly reported as stolen, according to research by MIT Technology Review.

Originally described as a "distributed ledger," blockchain makes forging a transaction difficult by employing a decentralized network of many users, or nodes, where each node stores an up-to-date copy of every transaction on the network. Protocols set the rules for how those transactions are verified. Each approved transaction is time-stamped, marked with a unique "hash"—a solved, complex equation—and locked into the chain; it's theoretically impossible to change one block of data without affecting all the others, which would be rejected by the network.

However, the very complexity that makes blockchain successful also opens new paths for error and abuse. Flawed protocols have occasionally been uncovered that permit approval of illegal transactions or allow them to occur without being recorded.

In other cases, bad actors have managed to gain control of at least 51 percent of the processing power of a blockchain network—this allows them to create a parallel version, a fork in the blockchain, and eventually convince the network to accept the false chain as authentic. Typically, the thieves will spend some cryptocurrency and then introduce a duplicate chain of transactions that skip that expenditure, allowing them to spend it again.

Such a "double spend" attack reported by Coinbase in January involved $1.1 million worth of the currency. Coinbase says no money was actually stolen from its accounts. Gaining 51 percent of the processing power of a network isn't easy—it's expensive, making large networks naturally less vulnerable. Yet instances of this type of attack are growing.

Another area of weakness involves "smart contracts," programs that run on a blockchain network for a variety of uses, including legal contracts and voting records. A bug in such a smart contract in the Ethereum blockchain allowed repeated requests for funds to go unrecorded—for a $60 million theft.

Because transactions in a blockchain cannot be undone, fixing such a bug can be a huge problem. To circumvent the Ethereum bug, the development community created a second blockchain, a fork based on a version of the old one that predated the flawed smart contract, and advised users to join that one. (Some still use the original, however, which is now called Ethereum Classic.) It's estimated that tens of thousands of smart contracts may contain some type of vulnerability.

The stakes for ever more sophisticated cyber security measures couldn't be higher. As society becomes more dependent on blockchain networks, these vulnerabilities—and others yet to be discovered—are certain to be exploited, fueled in part by the expanding number of eager, blockchain-fluent cyber engineers and the small percentage of them that stray to the dark side. ◆

CARLTON WILKINSON is the Managing Editor of the Brunswick Review and a Director with the firm, based in New York.

ILLUSTRATION: THOMAS FUCHS