# What Doesn't Kill the Blockchain Will Make It Stronger

By **Dmitry Stillermann**
August 3, 2016

A lot of debate is going on today around the Decentralized Autonomous Organization ("the DAO"). Some pessimists consider the situation around the DAO to be the proof that blockchain is a passing fad and will never be fit for use in financial markets. We believe that there are no fundamental problems with blockchain per se, that the mistakes were not really specific to blockchain and that the industry will use the whole experience to learn how to use blockchain properly.

The DAO was a self-governing investment community managing its assets solely through open and (supposedly) immutable rules embodied in software. It runs on top of Ethereum, a public blockchain platform — which recently split into two nearly identical versions — that aims to provide a programmable transaction functionality superior to bitcoin's. The key proclaimed benefit of the DAO was its reliance on smart contract technology for deal settlement, supposedly making it immune to human error and malice. Alas, relying on software did not protect the investments made into the DAO, as on June 17 a mysterious actor managed to find a loophole in the DAO's contracts and to siphon substantial amounts in ether, the cryptocurrency of Ethereum, out of the system.

This story is obviously pivotal for the future of all blockchain-based enterprises. Not surprisingly, most observers are extremely worried. There are some who say that the debacle demonstrates the blockchain as a whole to be a no-go. Others, while more optimistic, state those blockchain-based systems cannot deliver on their key promise — a completely decentralized environment where transaction execution and contract enforcement happen without involvement of any supreme authority. They say that we will always need human institutions outside the "system boundary" of blockchain to protect the interests of transacting parties. As Matt Levine wrote in his Bloomberg column, "Financial systems are supposed to work for humans. If the code rips off the humans,something has gone wrong."

Is such pessimism justified? We do not think so. Ironically, we believe that the most accurate description of these events is provided in the open letter published anonymously by the alleged "attacker," where he expresses hope that what's happened to the DAO will become a "valuable learning experience for the Ethereum community."

Virtually every technology poses numerous risks to its users — and doubly so when the technology is still in its infancy and the people have not yet learned how to work around those risks. Think of air travel, where the number of accidents steadily drops as the industry learns continuously from its own mistakes — and, unfortunately, paying for this learning in human casualties. Still, air travel has become an integral, irreplaceable part of our lives.

A much closer example can be found in the world of financial markets. The risks of complex derivatives, such as swap contracts or asset-backed securities, are notoriously difficult to calculate for a human mind unaided by advanced software. As the crisis of 2008 showed, these risks can

materialize unexpectedly — and yet, according to Bank of International Settlements, a whopping quadrillion dollars worth of derivatives were traded in the year 2015 (this is naturally a notional sum). If there are things humanity is especially good at, it's learning by trial and error.

How can blockchain technology evolve to make it safer for future users? First and foremost, creators of future DAOs need to take software quality seriously. It is illuminating that the same vulnerability that hit the DAO after its first funding round was duly discovered by Maker, another organization running on Ethereum blockchain. (It was promptly fixed without any material loss to anyone, as at the time of discovery Maker was still in the testing phase). This example shows that the underlying Ethereum platform was completely robust, but that the DAO founders got their software quality processes wrong. Dealing with money, especially other people's money, requires discipline, which does not occur automatically, but must be methodically implemented. Fortunately, the software industry is sufficiently mature to offer lots of best practices.

Given the importance of the smart contracts and the financial risks involved, we believe that the solution lies not in human oversight, but in objective testing and validation tools. Smart contracts are prime candidates for formal verification, one of the most advanced techniques in software quality assurance. Formal verification requires that the software be implemented in a language that has a strict specification of its semantics. Having this crystal-clear mathematical model allows to apply methods of logical proof to any piece of software written in this language to verify that it really does what it is supposed to do.

Formal verification is an established and respected area in computer science, but so far the designers of smart contract environments have been lax on this kind of formalities. Fortunately, some new implementations have begun to appear, incorporating the formal verification capability from the very beginning. The most promising is Tezos, whose smart contract language claims to be fully verifiable.

The recklessness of pioneers and the need for learning and discipline are nothing new and certainly not unique for the blockchain ecosystem. This ecosystem is currently living through turbulent yet fascinating early days. It is bound to become safer and more powerful, so we believe it is still a great time for experiments and investments into the future.

*Dmitry Stillermann is the vice president of the finance practice at DataArt, a technology consulting firm.*

Original article — http://www.americanbanker.com/bankthink/what-doesnt-kill-the-blockchain-will-make-it-stronger-1090554-1.html