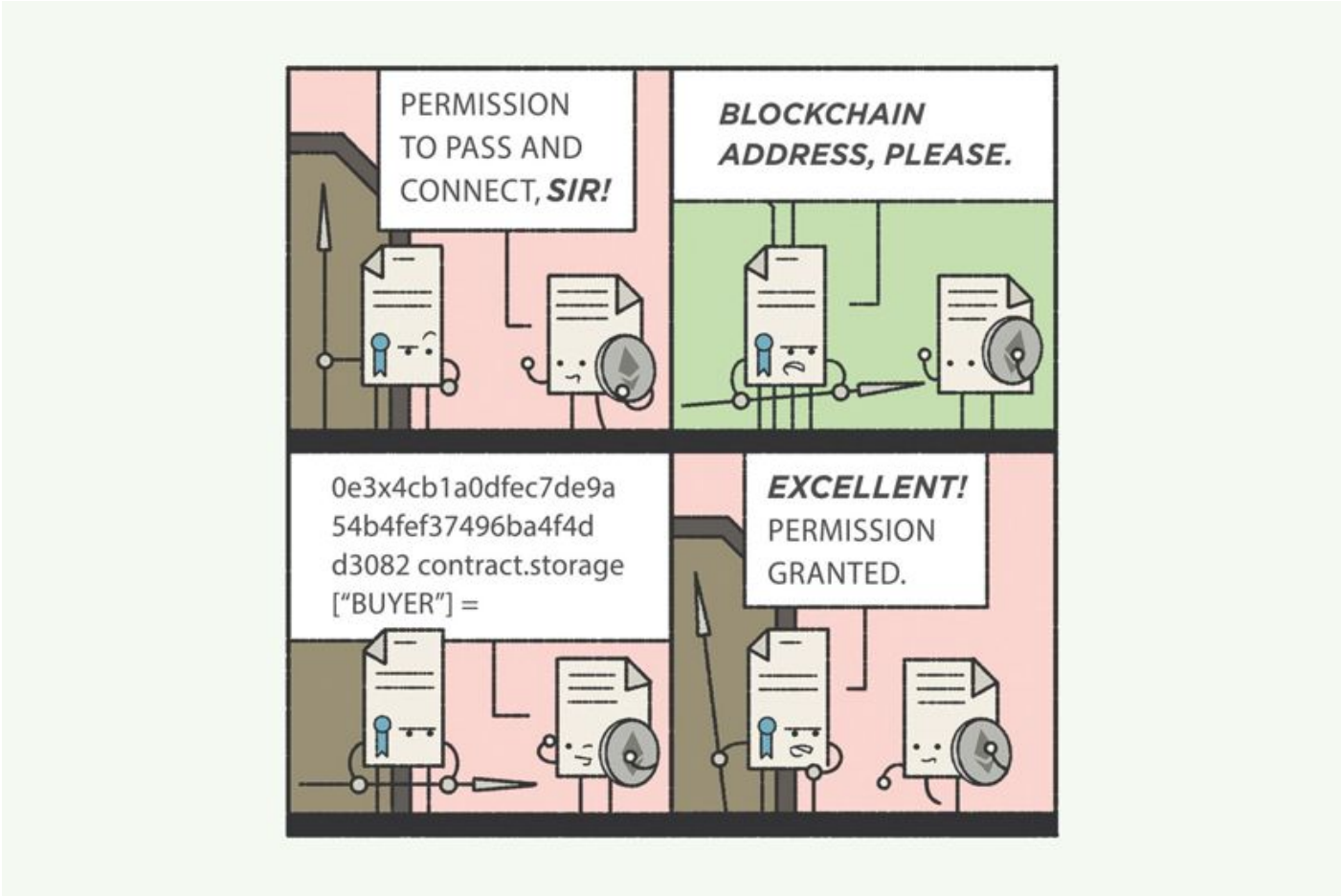
The WIRED World in 2017

The blockchain came after bankers and now it's going after lawyers

The increase in digital currencies mean future contracts will be vetted by hackers, not lawyers

By

05 Jan 2017



In the wake of the DAO's $50 million attack, it's time to bring the white-hat hackers on board

Credit **Nick D Burton**

We live in an increasingly automated economy where it seems there's no task that an app can't take care of. Over the past year, an international community of researchers, tech geeks and bankers has embarked on a series of projects to achieve what was once thought impossible: developing decentralised platforms where unstoppable, self-fulfilling programmable financial contracts called "smart contracts" can live.

A smart contract is like any other contract, whether it's for a mortgage, a loan, a job or an investment. The main difference is that the clauses are not written in English, secured by courts or executed by book-keepers. Instead, smart contracts are written in computer code, secured by cryptography and executed by an open network of computers that update a public ledger. The beauty of smart contracts is that the clauses execute themselves because they are computer code that runs on a public network, and so it's impossible to break their terms. No court system is needed.

What Yahoo can learn from LulzSec: reformed hacker reveals why transparency is key

Security | 20 Oct 2016

This is made possible by the blockchain, the ledger technology behind Bitcoin. Global banks such as Goldman Sachs, JP Morgan and Barclays are investing heavily, out of fear of getting left behind and being outpaced by lean startups. The technology opens the door for new breeds of financial products that are more efficient, democratic and secure than traditional finance. Smart contracts are doing to traditional contracts what smartphones did to dumb phones by unleashing a new world of life-changing permissionless innovation.

As with any big technological achievement, the success hasn't been without major

share to vote on investment proposals. The stated mission of the DAO is to "blaze a new path in business organisation for the betterment of its members, existing simultaneously nowhere and everywhere and operating solely with the steadfast iron will of unstoppable code".

However, the "unstoppable code" aspect of the DAO led to its downfall. On June 17, 2016, an anonymous attacker exploited an overlooked programming mistake in the code of the smart contract to which investors signed up, which allowed the attacker to freely withdraw $50m from the decentralised organisation's funds. This is similar to how a loophole in the law or a contract could allow someone to go against the intended spirit of it.

What ensued after the attack was a fierce philosophical debate within the community about how to proceed. Because of the intentional unstoppable design of Ethereum, the smart-contract platform on which the DAO runs on, there was nothing that anyone could do to reverse the attack. The platform operates on a global public network of computers that anyone can join. In order to break the rules of the system and return the stolen funds, you must convince a vast majority of users who run the computers in the network. This process is called a "hard fork", because it creates a split in the network to perform a fundamental change in the constitutional software rules running on computers maintaining the blockchain public ledger.

The line between politics and technology is blurring. Those pushing for a hard fork argued that social consensus trumps computer code because code exists to serve humans, and the interpretation of a contract should be its intended spirit rather than a loophole. In UK law this is what is referred to as reasonable terms in the Unfair Contract Terms Act 1977.

On the other hand, those pushing against a hard fork argued that it would be against the purpose of Ethereum, which is to be a "decentralised platform for applications that run exactly as programmed without any chance of fraud, censorship or third-party interference". A hard fork means third-party interference to stop an individual who fairly played by the rules of a contract that everyone signed up to.

After weeks of debate, a vote was put forward to the network that resulted in a majority of 87 per cent saying "Yes" to the hard fork. Incredibly, a $50 million theft

of damaging investor confidence, causing a rift in the community and potentially slowing down the pace of further innovation.

Perhaps this setback is what was needed to slow the rapid pace of change, so that essential safety features can be introduced to the system. One thing is for sure: as smart contracts become more commonplace, institutions are going to want to make sure they do as they're intended. And that means hiring white-hat hackers to write and review them.

Mustafa Al-Bassam is a former black-hat hacker who co-founded LulzSec. He now works as a security adviser at Secure Trading.

The WIRED World in 2017 *is WIRED's fifth annual trends briefing, predicting what's coming next in the worlds of technology, science and design*

This article was first published in the January 2017 issue of WIRED magazine

VIEW ISSUE

THE WIRED WORLD IN 2017 SECURITY HACKING BLOCKCHAIN

SHARE THIS ARTICLE

RECOMMENDED

By MATT KAMEN

Niantic | 01 Dec 2016

What's next for Solar Impulse? Pilots reveal where their iconic plane is going to take them now

By MATT BURGESS

Solar Power | 27 Jul 2016

Sony's PS4 4.5 update is out now. Here are its new features and how to download

By MATT KAMEN

Playstation VR | 09 Mar 2017

Minecraft: Education Edition is out now

By MATT KAMEN

Microsoft | 01 Nov 2016