

Can blockchain, a swiftly evolving technology, be controlled?

May 3 2017, by Vasilis Kostakis, Primavera De Filippi And Wolfgang Drechsler



Blockchain is an exciting technology, but for it to go mainstream governments must be able to regulate it. Credit: Name Coin/Flick

The headlong pace of technological change produces giant leaps forward in knowledge, innovation, new possibilities and, almost inevitably, legal



problems. That's now the case with blockchain, today's buzziest new tech tool.

Introduced in 2008 as the technology underpinning Bitcoin, a digital currency that is created and held electronically without any central authority, <u>blockchain</u> is a secure digital ledger for any kind of data. It simplifies record keeping and reduces transaction costs.

Its range of applications in commerce, finance and potentially politics continues to widen, and that has triggered a debate around how to regulate the tool.

Goodbye middleman

Because it does not require a centralised authority to verify and validate transactions, blockchain enables people who may not trust each other to interact and coordinate directly.

With blockchain, there is no middleman in peer-to-peer exchanges; instead, users rely on a decentralised network of computers that interact through a cryptographic, secure protocol.

Blockchain has the ability to "codify" transactions by deploying small snippets of code directly onto the blockchain. This code, generally referred to as a "smart <u>contract</u>", executes automatically when certain conditions are met.

An early example of smart contracts are the corporate-oriented digital rights management (DRM) systems limiting uses of digital files. Having DRM on your ebook may restrict access to copying, editing, and printing content.

With blockchain, smart contracts have become more complex and,



arguably, more secure. In theory, they will always be executed exactly as planned, since no one party has the power to alter the code binding a given transaction.

In practice, however, eliminating trusted brokers from a transaction can create some kinks.

One high-profile smart-contract failure happened to <u>the DAO</u>, a decentralised autonomous organisation for venture capital funding.

Launched in April 2016, the DAO quickly raised over US\$150 million via crowdfunding. Three weeks later, someone managed to exploit a vulnerability in the DAO's code, <u>draining approximately US\$50 million</u> worth of <u>digital currency</u> from the fund.

The security problem originated not in the blockchain itself but rather from issues with the smart-contract code used to administer the DAO.

Questions arose about the legality of the act, with some people arguing that since the hack was actually permitted by the smart-contract code, it was a perfectly legitimate action. After all, in cyberspace, "code is law".

The DAO debate raised <u>this key question</u>: should the intention of the code prevail over the wording of the code?

A new legal realm

<u>Blockchain proponents</u> envision a future in which entire companies and governments operate in a distributed and automated fashion.

But smart contracts pose a series of enforceability issues, which are outlined in a recent <u>white paper</u> by the London law firm Norton Rose Fulbright.



How can we resolve disputes arising over a self-executing smart contract? How do we identify what types of contractual terms can be properly translated into code, and which ones should instead be left to natural language? And is there a way combine the two?

It is not yet clear that code can address the necessary levels of complexity to replace legal language. After all, the vagueness inherent in the language of law is a feature, not a bug: it compensates for unforeseeable cases that must be assessed on a case-by-case basis in a court of law.

Traditional contracts acknowledge that no law can index the entire complexity of life as it is, let alone predict its future development. They also precisely define terms that can be enforced by law.

Smart contracts, by contrast, are simply snippets of code both defined and enforced by the <u>code</u> underpinning the blockchain infrastructure. Currently, they do not have any legal recognition. This means that when something goes wrong in a smart contract, parties have no legal recourse.

The DAO's founders painfully learned this lesson last year.

The creative friction of the law

If blockchain technologies are ever to go mainstream, governments will have to set up new legal frameworks to accommodate such complexities.

<u>Positive law</u> prescribes behaviour and penalises non-compliance. It can encapsulate the normative ideal that a respective government seeks to achieve, demonstrate an ethical vision for society or reify the power structure of the current regime.

Technological developments, on the other hand, are often oriented



toward profit and change.

There's an inherent tension here. Laws may delay the development of technology and hence hurt the competitive advantage of an entrepreneur or even a state.

Take the case of nanotechnology regulation in the European Union versus in the United States. European law so mitigates risks that it may end up limiting the technology's potential, losing its competitive edge against the US.

That's another fact about the law: slow and reactive, it can be a gross annoyance.

But ever since technological advances began speeding along on an exponential curve last century, the law has played a critical role in helping societies maintain certain previously negotiated standards for cohabitation.

Our legal system may sometimes seem antiquated in today's fast-moving world. But before changing our laws to accommodate new technologies that may (re)define our lives, it is important to have <u>room for debate and</u> <u>time for social struggles</u> to take place.

The law serves this function of creative friction. It can restore human agency against fierce technological development.

Given all the excitement over blockchain technologies, it is probable that interested parties will soon enough seek <u>legal recognition</u> and state-sanctioned enforceability of smart contracts.

These emerging technologies are still too new to have been subjected to a sufficiently thorough analysis of their social, economic and political



implications. More time is also needed to assess how blockchain could be deployed in a socially beneficial way.

Blockchain technology seems poised to constitute an important component of tomorrow's society. The legal system – slow-paced as it is – might be just what we need at this juncture to ensure that this new tool is deployed in a way consistent with established principles and values, with the common good at its core.

This article was originally published on <u>The Conversation</u>. Read the <u>original article</u>.

Provided by The Conversation

Citation: Can blockchain, a swiftly evolving technology, be controlled? (2017, May 3) retrieved 28 April 2024 from https://techxplore.com/news/2017-05-blockchain-swiftly-evolving-technology.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.