

OPINION

The transformative nature of blockchain-based smart contracts

By Emir Hrnjic and Nikodem Tomczak

As well as providing the backbone of cryptocurrencies such as Bitcoin and Ether, the emergence of blockchain technology has enabled a range of other lesser-known technological advances.

One such development is the emergence of so-called smart contracts – an application that some advocates believe could prove to be even more transformative.

On the surface, smart contracts work like traditional contracts, outlining the terms of an agreement between two or more parties. The “smart” element supposedly comes from the cryptographic code that verifies, executes and enforces the terms of the agreement.

The value of smart contracts lies in the ability to automate the execution of a range of tasks when predefined conditions are met. As smart contracts are typically self-verifying, self-executing and self-enforcing, they do not require an intermediary or a central authority to regulate the contract’s execution. With no need for a middleman, the predictable nature of the code that underpins them drastically reduces the cost of doing business.

In addition, the code of smart contracts can be easily audited by all parties involved while the blockchain provides a tamper-proof record of every transaction executed.

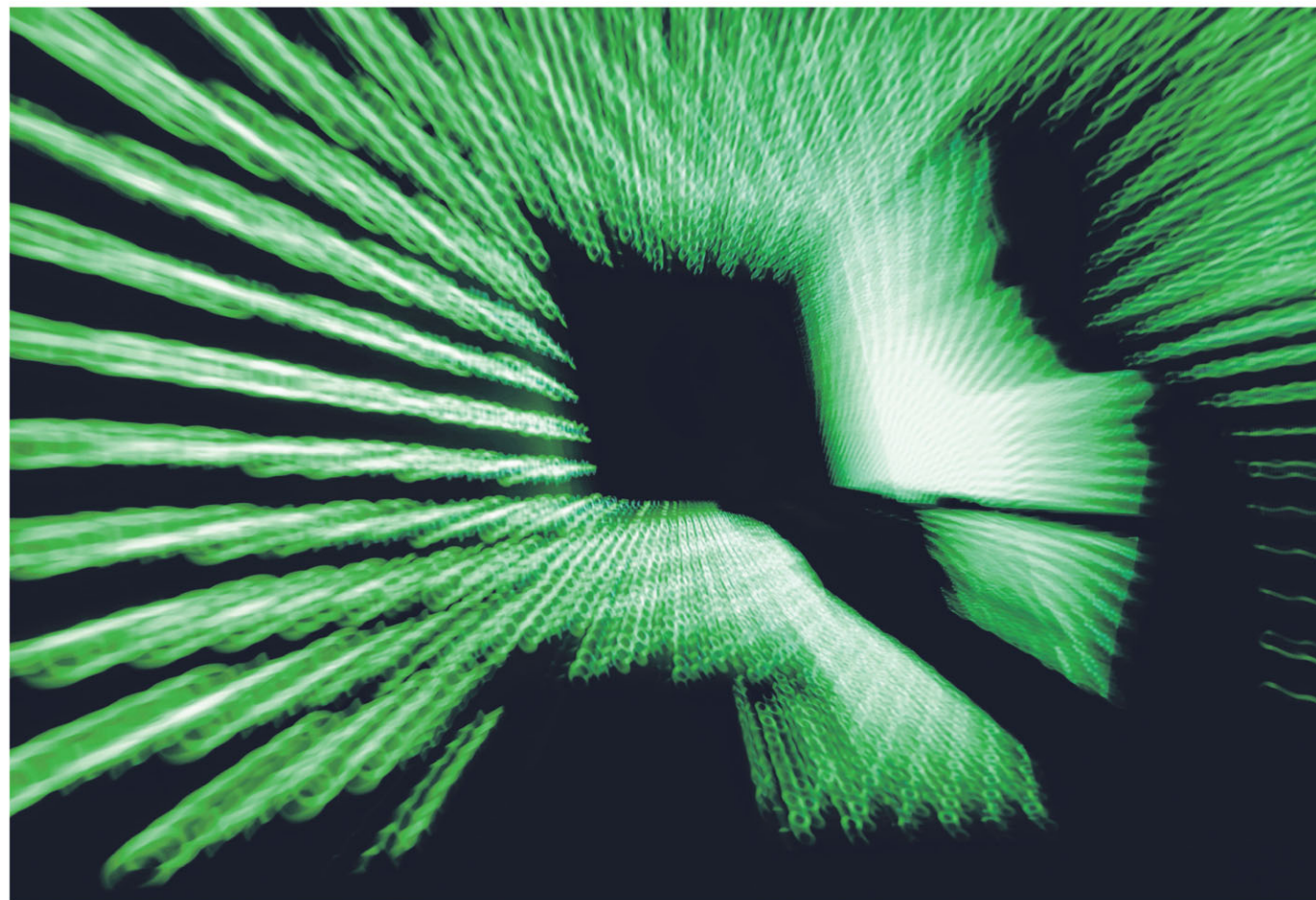
Yet, regardless of how conceptually powerful smart contracts may be, it could also be argued that they are neither “smart” nor “contracts”.

Indeed, they are only as reliable as the code describing them and the blockchain that secures them against manipulation. While simple agreements could be automated, more sophisticated contracts are more likely to require human judgment or off-blockchain resolution of disputes.

The immutable nature of blockchain technology is typically celebrated for its positive implications, but this same feature also has the potential to cause adverse effects and increased risk. For example, the computer code that underpins them is susceptible to human error as much as a written contract.

Furthermore, just because the smart contracts are enforceable on the level of computer code, it does not necessarily mean that they are legally binding agreements.

In fact, it is highly debatable whether the nature of the code describing contract provisions constitutes legally enforceable obligations unless some of the provisions are moved outside the blockchain. In other words, it is un-



The immutable nature of blockchain technology is typically celebrated for its positive implications, but this same feature also has the potential to cause adverse effects and increased risk. BT FILE PHOTO

clear whether transacting parties need real-world legal agreements in addition to smart contracts on blockchain.

In an effort to clarify this and attract businesses and investors, the US state of Arizona and several other states have recently passed bills recognising the legal effect of smart contracts in conducting electronic transactions, helping to pave the way for their wider acceptance as standard business practice.

The applications of smart contracts range from simple data storage to complex accountancy, finance and governance frameworks. They have served as the basis for development of decentralised applications enabling the initiation, funding and servicing of loans. And, for better or worse, they have enabled the creation of a range of

crypto-tokens, serving as the backbone of initial coin offerings (ICOs).

Smart contracts are poised to transform the finance sector by automating loans, insurance and payments, drastically reducing overhead costs and increasing efficiency. Transparent recording of transactions and auditable contract code reduce the likelihood of disputes and hence accelerate financial transactions involved.

However, we have also seen that vulnerabilities in smart contracts can lead to major losses of funds.

In one infamous example in 2016, a hack exploited weakness of smart contracts underpinning The DAO, a blockchain-enabled venture capital fund, causing a loss of 3.6 million Ether (the equivalent of roughly US\$50 million at the time).

The funds were ultimately recovered as developers opted to reset Ethereum’s codebase. However, this came at a major reputational cost, since Ethereum’s blockchain history was rewritten, casting into question the supposed decentralisation and immutability of the platform.

Despite this, smart contracts continue to find new applications. The recording and publishing industries, for example, are beginning to use smart contracts to enforce copyright and tackle piracy and plagiarism, thus preventing potential multimillion-dollar losses.

So, while blockchain-based smart contracts are relatively new, their rapid rise and breadth of application shows a degree of confidence in their future.

Indeed, their transformative effect

The value of smart contracts lies in the ability to automate the execution of a range of tasks when predefined conditions are met. As smart contracts are typically self-verifying, self-executing and self-enforcing, they do not require an intermediary or a central authority to regulate the contract’s execution.

could mean that smart contracts may become an entire industry in itself, underpinning a new decentralised finance sector.

However, for smart contracts to achieve wider adoption, the industry will have to overcome some key hurdles. One of the main shortcomings is concerns about the fragile state of cyber security, as potential adopters worried about possible loss of funds may choose to stay on the sidelines and wait for improved solutions.

Likewise, unscrupulous developers remain a danger to the industry, despite regulators around the world increasing the scrutiny and prosecution of illegal practices. Unclear legal ramifications, meanwhile, increase the uncertainty and risk to potential adopters.

In the meantime, blockchain developers will have to work hard to close the vulnerabilities in code, lawyers must fully understand and prepare for the legal repercussions, and entrepreneurs should figure out what role smart contracts can play in defining the future of their business.

■ The writers are from the National University of Singapore. Emir Hrnjic is a visiting senior research fellow at the Centre for Asset Management & Research Investment (CAMRI) at NUS Business School; Nikodem Tomczak is a research scientist and adjunct associate professor. Both are co-founders of Block’N’White. The opinions expressed are the writers’ and do not represent the views and opinions of NUS.

► More opinions and views, Pages 20-21