COMMENT

ANTONIO ZAMBARDINO/CONTRASTO/EYEVINE

To improve food traceability, some Indonesian fishermen have logged sustainably caught fish on the blockchain in a trial with UK firm Provenance.

The environment needs cryptogovernance

The blockchain technology that underpins cryptographic currencies can support sustainability by building trust and avoiding corruption, explains **Guillaume Chapron**.

Today's modes of governance are prone to corruption and are unable to steer humanity towards sustainability, despite the ongoing global environmental crisis. A technological innovation triggered by another crisis — the 2008 financial meltdown — offers radical solutions.

Bitcoin, an open-source virtual currency, or 'cryptocurrency', was launched by an anonymous developer in 2008 as a way to trade without banks, which were failing. Bitcoin's total market worth exceeds US$28 billion — greater than large companies such as Renault. The Bitcoin currency is completely secure because it uses a digital protocol that relies on cryptography: the blockchain. This ledger keeps track of all Bitcoin transactions. No central authority controls the blockchain — its operation is distributed across many computer platforms around the world.

Bitcoin's strength lies in how it approaches trust. Instead of checking the trustworthiness of each party, the system assumes that everyone behaves selfishly. No matter how greedily traders act, the blockchain retains integrity and can be trusted even if the parties cannot. Bitcoin demonstrates that banks and governments are unnecessary to ensure a financial system's reliability, security and auditability[1].

The arrival of the blockchain has been compared to the invention of double-entry book-keeping (first described in print in the fifteenth century by Italian mathematician Luca Pacioli), which enabled the modern economy. I think that its implications reach far beyond finance, to governance and sustainability. ▶

Lawyers guarantee contracts and states guarantee the rule of law in the same way as central banks guarantee currencies. Governing institutions need to establish trust between individuals, groups, firms and societies. If humans repeatedly fail to build trust, perhaps algorithms should replace them. The environmental crisis is growing partly because of a lack of trust — the increasing distance between multiple actors who are unknown to each other, from companies and governments to individual consumers, creates many opportunities for fraud and failed policies. The time is ripe for 'cryptogovernance', in which trust, law and enforcement are outsourced to computer code.

For sustainability, blockchain technology could be a game-changer. It can generate trust where there is none, empower citizens and bypass central authorities. It could also make existing institutions obsolete, including governments, and raise fierce opposition. Laws could be replaced with 'smart contracts' written in computer code.

UNIQUE RECORD

The blockchain proves with certainty that a recorded piece of information — a piece of data, document, transaction, certificate, event or identity — existed at a particular time. If an asset can be assigned a unique digital identifier, such as a barcode, then it can be included (see 'Blockchain governance').

That identifier is run through a cryptographic function that turns it into a unique string of numbers and letters, called a hash; this is stored in the blockchain. The hash can be recalculated later to prove that the asset existed at a particular time. There is no need to reveal the asset itself. For example, the start-up firm Proof of Existence uses the blockchain to certify and timestamp digital documents, such as official certificates like diplomas, or scientific or medical data.

The hashing function operates only in one direction — the hash value does not allow you to go back and obtain the original document that generated it, and you cannot guess which document will give you a particular hash value. This means that Bitcoin certificates cannot be forged. The system says nothing about the veracity of the data or documents registered; this must be assessed by other means. For instance, the identities and reputations of human assessors can be assured using cryptographic key infrastructure, meaning that only certified and reputable assessors can enter data. And data generated automatically from sensors — such as radio frequency identification chips or sensors for temperature or water quality — can be hashed and fed directly into the blockchain.

Blockchain technology can guarantee that a planned event will happen. For example, an invoice will be automatically paid when a shipment arrives[1]. This is done by drawing up 'smart contracts' that represent business logic written in computer code. That code is implemented on the blockchain using a programming extension called Ethereum[2]. Smart contracts execute when particular conditions are met. Barclays corporate banking arm is prototyping their use in financial services, for example.

Smart contracts have many advantages. Their execution is independent of the will, approval or actions of the parties involved, and it is impossible to withdraw from them. They require no trusted third party or escrow document to manage them. They are cheap. Computer code has less ambiguity than natural languages. And they are independent of existing legal rules or institutions.

Smart contracts could be used to set up autonomous digital entities to manage natural resources[3]. For example, a quota for extracting natural resources could be issued to a community only after remote sensing data have proved that the community has met conservation targets. This natural resource would be stamped with a sustainability certificate that permits the community to access a market for these certified products.

"Blockchain technology can guarantee that a planned event will happen."

FOUR WINS

At least four areas related to governance and sustainability could benefit from using the blockchain.

Ownership. From a birth certificate to a fish or a forest, the blockchain can certify the existence and ownership of anything that can be digitalized. For example, a certificate stating a community owns a forest can be logged in the blockchain with a time stamp. The certificate's authenticity can be proved by showing a document that returns the same hash. Start-up companies are beginning to do this — the firm Benben in Accra is developing land-title registries for Ghana using the blockchain, and Georgia and Honduras are doing the same. This could limit the eviction of local populations by industries or corrupt governments.

Traceability. Physical goods can be traced throughout their life cycle. The start-up firm Everledger in London certifies and tracks trade in diamonds, to reduce sales of stolen gems or conflict stones from warlords. The technology platform Provenance, also in London, is developing a blockchain-based protocol to track resources and materials. It worked with the Indonesian fishing industry last year to trace sustainably caught fish along the supply chain. Minerals, wood or food could similarly be followed. Customs officials could spot illegally traded animal parts or plants by using portable DNA barcode scanners.

Other commodities could have their ecological footprints tagged in the blockchain if the footprint were linked to the Internet of Things, with sensors recording the environmental impacts of manufacturing processes. Walmart is tracking its pork supply chain in China by recording information such as farm origin and storage temperature in the blockchain. Companies could also track how much water, energy or raw material they use. The overall environmental impact of firms or consumers could be recorded on the blockchain and sustainable behaviour rewarded through incentives such as tax rebates. Building a life-cycle record of goods would also help to develop the circular economy.

Incentives. Two billion adults worldwide lack banking services. The blockchain could allow them to enter the financial economy: bitcoins can be transferred without a bank account. Communities that have rights to natural resources could receive direct payments in bitcoins for ecosystem services or for meeting conservation targets. Healthy ecosystems could replace other forms of capital storage, such as cattle.

The blockchain could ensure that conservation and development funding is used as intended. Money can be tracked, attached to a specific purpose, have an expiry date or be released when project milestones are met. Funds cannot be siphoned off. Middlemen are cut out.

The blockchain makes it easier to collect insurance against, say, crop damage by wildlife. Payments are immediate, minimizing delay or corruption, although clerks are still needed to assess the damages. Communities could trade renewable energy through the blockchain affordably, quickly and reliably without being controlled by a third party. An Ethereum-based trading platform for carbon credits was launched in March 2017 on the Russian carbon market by a climate finance group.

Policymaking. The blockchain will disrupt all institutions, including governments[4]. A public, shared and immutable register of assets and transactions can help the public to hold politicians accountable. Authorities cannot withdraw or forge evidence, nor seize or shut down blockchain-based institutions.

Votes may be cast as transactions[5]. Blockchain voting has been used by a South Korean community government in a local budget ballot. It is also being implemented for a Danish political party's internal elections, and for shareholders of NASDAQ companies listed on the Tallinn stock

exchange. The postal service Australia Post is looking into using it for university and civic elections. The city of Moscow is exploring applying the blockchain to bypass voting fraud. Local communities could be empowered to manage their natural resources through ad hoc voting. For example, fish might be traded on a platform only if harvest quotas were approved by a community-based democratic process.

The blockchain can revolutionize the 'sharing economy' by giving control back to users. For example, smart contracts between individual taxi drivers and passengers could replace app-based systems such as the taxi service Uber. An agreed payment for transporting someone would be delivered only when the passenger reached their desired point, and the driver would know before picking the person up that they have the funds to pay. As Vitalik Buterin, founder of the Ethereum blockchain, said: "Instead of putting the taxi driver out of a job, blockchain puts Uber out of a job and lets the taxi drivers work with the customer directly"[1].

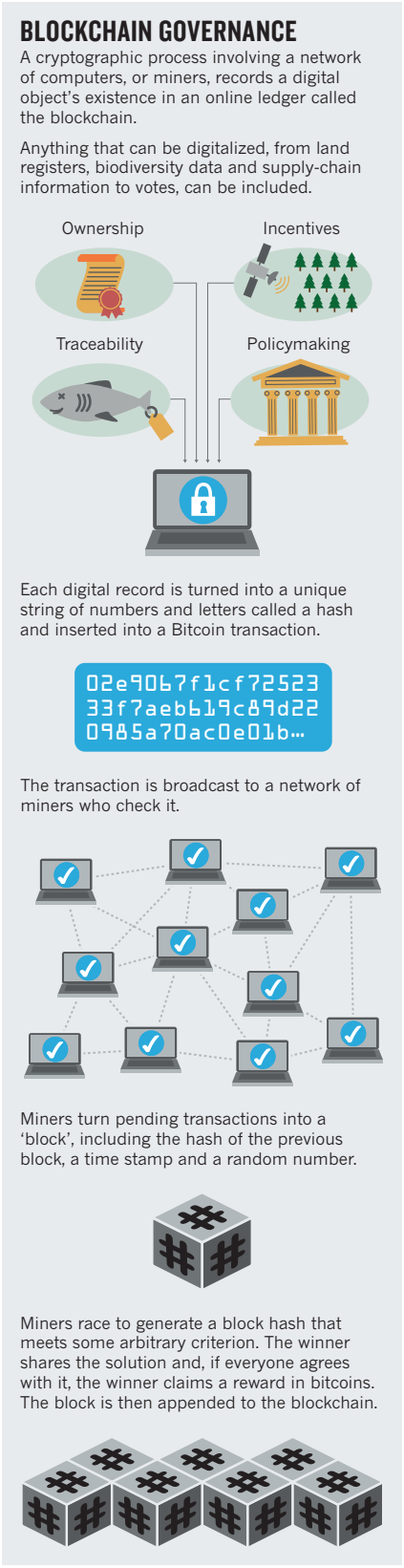
TECHNICAL CHALLENGES

There are obstacles. Bitcoin is slow: it is limited to 7 transactions per second, compared with an average of 2,000 transactions per second for the Visa credit network[6]. To run and check its complex algorithms, Bitcoin requires a network of dedicated 'mining farms' of high computing power, most of which are based in China, Georgia, the United States, Canada and Sweden (see also *Nature* **526,** 21–23; 2015). These use a comparable amount of electricity to whole cities[7]. Bitcoin is estimated to consume about 10.4 terawatt hours a year[7], almost twice that used by Google as a company (5.7 TWh).

Like any emerging technology, the blockchain will take time and encouragement to be adopted. Simple applications, such as storing value in coins, will be taken up sooner than complex ones, such as setting up autonomous digital organizations[8]. In its favour is the ubiquity of smartphones: for instance, 43% of Kenya's gross domestic product is now spent through mobile phones. But the benefits and risks of Bitcoin will be hard for people to understand, because the technology is complicated. If you lose your cryptographic key to a Bitcoin wallet there is no way to recover the coins, and no one to turn to.

Some governments and institutions will undoubtedly resist the blockchain fiercely, once they realize its disruptive potential. However, it is also a tool to increase efficiency and economic growth. And it is now too late to ban Bitcoins. Even with the blockchain, governance will remain political. For instance, the choice to use it promotes a certain world view, in which the central authority of the state is transferred to a decentralized consensus of computers.

Blockchain law, in the form of a set of 'if-then-else' instructions, may emerge as a legal system in its own right, alongside common and civil law. It will be challenging to work out how the different legal systems can interact. Legal languages are nuanced and must be interpreted by trained lawyers; programming languages consist of unambiguous machine instructions. Courts are unlikely to understand computer code. And programmers may not understand the real-world implications of their code. Although the lifetime of smart contracts can be limited, computational laws cannot be stopped or unplugged, and are enforced regardless of their consequences[9].



SOURCE: G. CHAPRON

NEXT STEPS

Blockchain technology is already entering segments of the economy. Sustainability should become one of them.

Sustainability scientists and blockchain developers must meet and discuss problems and solutions. Funding agencies should encourage 'SusTech' proposals for technology that blends cryptography and sustainability. Researchers need to find more energy-efficient mechanisms for Bitcoin mining. Psychological research is needed into people's trust of technology in the context of cryptography. Most importantly, programmers and lawyers must collaborate on formulating smart contracts. Dictionaries will be needed that link legal languages and computer codes.

It is time for blockchain governance. It could benefit people and help societies to become sustainable. ■

Guillaume Chapron *is associate professor in ecology at the Grimsö Wildlife Research Station, Department of Ecology, Swedish University of Agricultural Sciences, Riddarhyttan, Sweden; and senior research associate at the Wildlife Conservation Research Unit, Recanati-Kaplan Centre, Department of Zoology, University of Oxford, Tubney, UK.*
e-mail: guillaume.chapron@slu.se

1. Tapscott, D. & Tapscott, A. *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World* (Portfolio, 2016).
2. Dannen, C. *Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners* (Apress, 2017).
3. Raval, S. *Decentralized Applications: Harnessing Bitcoin's Blockchain Technology* (O'Reilly Media, 2016).
4. Reijers, W., O'Brolcháin, F. & Haynes, P. *Ledger* **1,** 134–151 (2016).
5. Lee, K., James, J. I., Ejeta, T. G. & Kim, H. J. *J. Digit. Forensics Secur. Law* **11,** 123–136 (2016).
6. Mougayar, W. *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology* (Wiley, 2016).
7. Hileman, G. & Rauchs, M. *Global Cryptocurrency Benchmarking Study* (Cambridge Centre for Alternative Finance, 2017); available at http://go.nature.com/2pofnyz
8. Iansiti, M. & Lakhani, K. R. *Harvard Bus. Review* **95,** 119–127 (2017).
9. Narayanan, A., Bonneau, J., Felten, E., Miller, A. & Goldfeder, S. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction* (Princeton Univ. Press, 2016).