CHRIS RYAN/NATURE

# BITCOIN AND BEYOND

*The digital currency has caused any number of headaches for law enforcement. Now entrepreneurs and academics are scrambling to build a better version.*

**BY ANDY EXTANCE**

When the digital currency Bitcoin came to life in January 2009, it was noticed by almost no one apart from the handful of programmers who followed cryptography discussion groups. Its origins were shadowy: it had been conceived the previous year by a still-mysterious person or group known only by the alias Satoshi Nakamoto[1]. And its purpose seemed quixotic: Bitcoin was to be a 'cryptocurrency', in which strong encryption algorithms were exploited in a new way to secure transactions. Users' identities would be shielded by pseudonyms. Records would be completely decentralized. And no one would be in charge — not governments, not banks, not even Nakamoto.

Yet the idea caught on. Today, there are some 14.6 million Bitcoin units in circulation. Called bitcoins with a lowercase 'b', they have a collective market value of around US$3.4 billion. Some of this growth is attributable to criminals taking advantage of the anonymity for drug trafficking and worse. But the system is also drawing interest from financial institutions such as JP Morgan Chase, which think it could streamline their internal payment processing and cut international transaction costs. It has inspired the creation of some 700 other cryptocurrencies. And on 15 September, Bitcoin officially came of age in academia with the launch of *Ledger*, the first journal dedicated to cryptocurrency research.

What fascinates academics and entrepreneurs alike is the innovation at Bitcoin's core. Known as the block chain, it serves as the official online ledger of every Bitcoin transaction, dating back to the beginning. It is also the data structure that allows those records to be updated with minimal risk of hacking or tampering — even though the block chain is copied across the entire network of computers running Bitcoin software, and the owners of those computers do not necessarily know or trust one another.

Many people see this block-chain architecture as the template for a host of other applications, including self-enforcing contracts and secure systems for online voting and crowdfunding. This is the goal of Ethereum, a block-chain-based system launched in July by the non-profit Ethereum Foundation, based in Baar, Switzerland. And it is the research agenda of the Initiative for CryptoCurrencies and Contracts (IC3), an academic consortium also launched in July, and led by Cornell University in Ithaca, New York.

Nicolas Courtois, a cryptographer at University College London, says that the Bitcoin block chain could be "the most important invention of the twenty-first century" — if only Bitcoin were not constantly shooting itself in the foot.

Several shortcomings have become apparent in Bitcoin's implementation of the block-chain idea. Security, for example, is far from perfect: there have been more than 40 known thefts and seizures of bitcoins, several incurring losses of more than $1 million apiece.

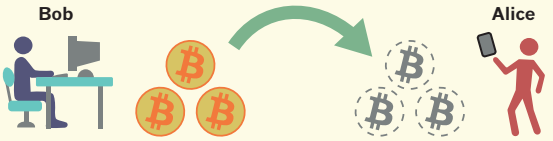
Cryptocurrency firms and researchers are attacking the problem with tools such as game theory and advanced cryptographic methods. "Cryptocurrencies are unlike many other systems, in that extremely subtle mathematical bugs can have catastrophic consequences," says Ari Juels, co-director of IC3. "And I think when weaknesses surface there will be a need to appeal to the academic community where the relevant expertise resides."

# THE BITCOIN GAME

The cybercurrency's **mining** process is designed to produce a secure online ledger of every Bitcoin transaction — even though no one is in charge.

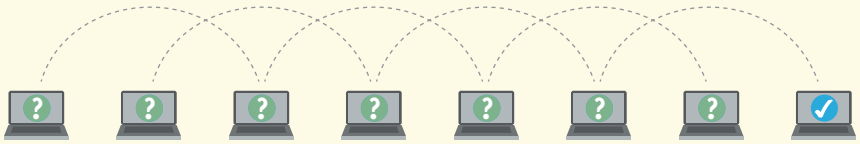
## THE TRANSACTION

Bob sends some bitcoins to Alice, both use pseudonyms to keep their identities secret.



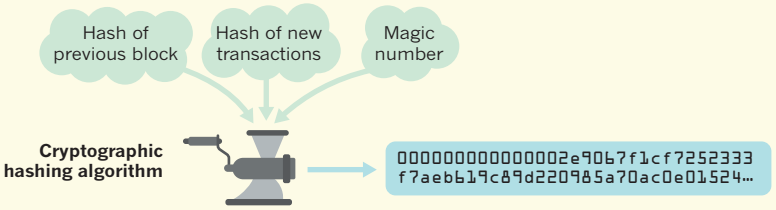

## THE MINERS

Digital copies of the transaction are passed to **miners** for verification.
The miners are individuals or groups running the **Bitcoin software** in a worldwide network of independent computers. They compete to turn the latest transactions into a **block**. Roughly every ten minutes, one of them succeeds.



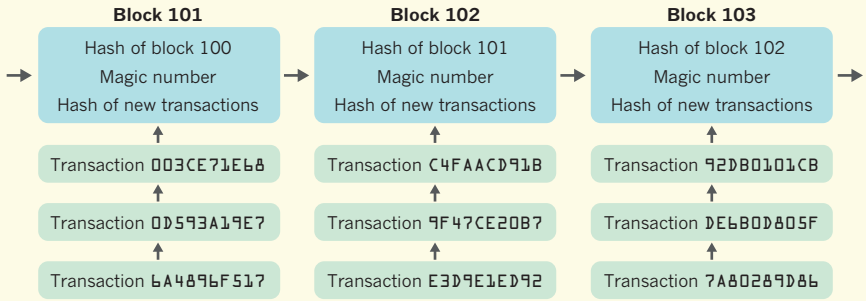
## THE WINNING BLOCK

Encrypting the transactions creates a **hash** — a seemingly random sequence of numbers and letters.
The miners try to find a **magic number** that when encrypted alongside the transactions and the most recent block in the chain creates a hash that starts with a particular number of zeros.
Although this number is very hard to find, once a solution has been found it can be verified easily by the other miners. The first miner to solve the problem is rewarded with bitcoins, and the block is added to the **block chain**.




## THE BLOCK CHAIN

The block chain is an online ledger that records every Bitcoin transaction ever made.
A copy of the block chain is held by each miner and it is used as proof of ownership for all bitcoins.
Chronological order is very important in the chain. If Bob has already spent his bitcoins elsewhere it will be recorded in the block chain and his transfer to Alice will be rejected.




SOURCE: BITCOIN.ORG

Academic interest in cryptocurrencies and their predecessors goes back at least two decades, with much of the early work spearheaded by cryptographer David Chaum. While working at the National Research Institute for Mathematics and Computer Science in Amsterdam, the Netherlands, Chaum wanted to give buyers privacy and safety. So in 1990 he founded one of the earliest digital currencies, DigiCash, which offered users anonymity through cryptographic protocols of his own devising.

DigiCash went bankrupt in 1998 — partly because it had a centralized organization akin to a traditional bank, yet never managed to fit in with the financial industry and its regulations. But aspects of its philosophy re-emerged ten years later in Nakamoto's design for Bitcoin. That design also incorporated crowdsourcing and peer-to-peer networking — both of which help to avoid centralized control. Anyone is welcome to participate: it is just a matter of going online and running the open-source Bitcoin software. Users' computers form a network in which each machine is home to one constantly updated copy of the block chain.

Nakamoto's central challenge with this wide-open system was the need to make sure that no one could find a way to rewrite the ledger and spend the same bitcoins twice — in effect, stealing bitcoins. His solution was to turn the addition of new transactions to the ledger into a competition: an activity that has come to be known as mining (see 'The Bitcoin game').

Mining starts with incoming Bitcoin transactions, which are continuously broadcast to every computer on the network. These are collected by 'miners' — the groups or individuals who choose to participate — who start competing for the right to bundle transactions into a new block. The winner is the first to broadcast a 'proof of work' — a solution showing that he or she has solved an otherwise meaningless mathematical puzzle that involves encrypted data from the previous block, and lots of computerized trial and error. The winning block is broadcast through the Bitcoin network and added to the block chain, with the proof of work providing an all but unbreakable link. The block chain is currently almost 400,000 blocks long.

In principle, this competition keeps the block chain secure because the puzzle is too hard for any one miner to solve every time. This means that no one will ever gain access to the encrypted links in the block chain and the ability to rewrite the ledger.

Mining is also a way to steadily increase the bitcoin supply: the miner who wins each block gets a reward, currently 25 new bitcoins. That is worth almost $6,000 at today's prices. Nakamoto's design controls the supply increase by automatically adjusting the difficulty of the puzzle so that a new block is added roughly every ten minutes. In addition, the reward for creating a block decreases by half roughly every four years. The goal is to limit the supply to a maximum of 21 million bitcoins.

The network cannot determine the value of bitcoins relative to standard currencies, or real-world goods and services. That has been left to market forces, with people trading bitcoins on online exchanges. One result is that the market price has gyrated spectacularly — especially in 2013, when the asking price soared from $13 per bitcoin in January to around $1,200 in December. That would have made the first real-world products ever paid for with the cryptocurrency — a pair of Papa John's pizzas, purchased for 10,000 bitcoins on 22 May 2010 — worth almost $12 million.

## PUZZLE SOLUTIONS

It did not take long for the problems with Bitcoin to become apparent. For example, because users are allowed to mask their identity with pseudonyms, the currency is perfect for screening criminal activity. That was behind the success of the online black market Silk Road, which the FBI shut down in 2013; its founder was sentenced to life in prison in May this year. But Bitcoin also had a key role

in funding the whistle-blowing website WikiLeaks — an outcome that some would call beneficial. It is difficult for society to work out a legal framework to differentiate between good and bad uses of this technology, says Arvind Narayanan, a computer scientist at Princeton University in New Jersey. "How do you regulate around Bitcoin without banning the technology itself?" he asks.

Other issues surfaced with Bitcoin's mining procedure. As the currency has gained value, for example, mining competition has become fiercer, with increasingly specialized computers solving the puzzles ever faster. Courtois, who has found ways to streamline the puzzle-solving process[2], says that at one point he was successfully earning $200 a day through mining. The rivalry has driven the establishment of large Bitcoin-mining centres in Iceland, where cooling for the computers is cheap. According to one estimate from 2014, Bitcoin miners collectively consumed as much power as the whole of Ireland[3].

## WORKING TOGETHER

Intensified Bitcoin mining has also led individual miners to pool their computational resources. Last year, the largest mining pool, GHash.IO, briefly exceeded 50% of total Bitcoin mining power — which is problematic because anyone who controls more than half of the mining power could start beating everyone else in the race to add blocks. This would effectively give them control of the transaction ledger and allow them to spend the same bitcoins over and over again. This is not just a theoretical possibility. Successful '51% attacks' — efforts to dominate mining power — have already been mounted against smaller cryptocurrencies such as Terracoin and Coiledcoin; the latter was so badly damaged that it ceased operation.

To reduce the threat from mining pools, some existing cryptocurrencies, such as Litecoin, use puzzles that call more on computer memory than on processing power — a shift that tends to make it more costly to build the kind of specialized computers that the pools favour. Another approach, developed by IC3 co-director Elaine Shi and her collaborators[4], enlists a helpful kind of theft. "We are cryptographically ensuring that pool members can always steal the reward for themselves without being detected," explains Shi. Their supposition is that miners would not trust each other enough to form into pools if their fellow pool members could easily waltz off with the rewards without sharing. They have built a prototype of the algorithm, and are hoping to see it tested in Bitcoin and other cryptocurrencies.

Another problem is the profligate amount of electricity used in Bitcoin mining. To reduce wastage, researchers including Shi and Juels have proposed a currency called Permacoin[5]. Its proof of work would require miners to create a distributed archive for valuable data such as medical records, or the output of a gene-sequencing centre. This would not save energy, but would at least put it to better use.

**➲ NATURE.COM**
To hear more about cryptocurrencies:
go.nature.com/icc8kv

The security of cryptocurrencies is another huge concern. The many thefts of bitcoins do not result from the block-chain structure, says Narayanan, but from Bitcoin's use of standard digital-signature technology. In digital signatures, he explains, people have two numeric keys: a public one that they give to others as an address to send money to, and a private one that they use to approve transactions. But the security of that private key is only as good as the security of the machine that stores it, he says. "If somebody hacks your computer, for example, and steals your private keys, then essentially all of your bitcoins are lost."

Security is such a concern for consumers that Narayanan thinks Bitcoin is unlikely to find widespread use. So his team is working on a better security scheme that splits private keys across several different devices, such as an individual's desktop computer and smartphone, and requires a certain proportion of the fragments to approve a payment[6]. "Neither reveals their share of the key to each other," says Narayanan. "If one machine gets hacked, you're still OK because the hacker would need to hack the others to steal your private key. You'll hopefully notice the hack happened before they have the chance."

Other thefts have occurred because the private key needs to be combined with a random number to create a transaction signature. Some software — such as Bitcoin apps developed for Android smartphones — has generated random numbers improperly, making them easier to guess. This has allowed hackers to steal somewhere between several thousand and several million dollars' worth of bitcoins, says Courtois, who has been investigating such vulnerabilities[7]. "It's embarrassing," admits David Schwartz, chief cryptographer at cryptocurrency developer Ripple Labs in San Francisco, California. "We as an industry just seem to keep screwing up."

## INTO THE ETHER

The block chain is a remarkably powerful idea that could be applied to much more than just transaction records, says Gavin Wood, co-founder of Ethereum and chief technology officer of its foundation. One use might be to develop computerized, self-enforcing contracts that make a payment automatically when a task is complete. Others might include voting systems, crowdfunding platforms, and even other cryptocurrencies. Wood says that Ethereum is best used in situations for which central control is a weakness — for example, when users do not necessarily trust one another. In 2014, to make it easier to develop such applications, Wood and fellow programmer Vitalik Buterin devised a way to combine the block chain with a programming language. Ethereum raised 30,000 bitcoins through crowdfunding to commercialize this system.

To prevent the basic cryptography-related mistakes that have plagued Bitcoin, Ethereum has recruited academic experts to audit its protocol. Shi and Juels are looking for ways that Ethereum could be abused by criminals[8]. "The technology itself is morally neutral, but we should figure out how to shape it so that it can support policies designed to limit the amount of harm it can do," says Juels.

Like Bitcoin, Ethereum is not under anyone's direct control, so it operates outside national laws, says Wood. However, he adds that technologies such as music taping and the Internet were also considered extralegal at first, and seemed threatening to the status quo. How Bitcoin, Ethereum and their successors sit legally is therefore "something that, as a culture and society, we're going to have to come together to deal with", he says.

Juels suspects that Bitcoin, at least, will not last as an independent, decentralized entity. He points out how music streaming has moved from the decentralized model of peer-to-peer file-sharing service Napster to commercial operations such as Spotify and Apple Music. "One could imagine a similar trajectory for cryptocurrencies: when banks see they're successful, they'll want to create their own," he says.

Courtois disagrees. He calls Bitcoin "the Microsoft of cryptocurrency", and maintains that its size and dominance mean that it is here to stay. As soon as any new innovations come along, he suggests, Bitcoin can adopt them and retain its leading position.

Whatever the future holds for Bitcoin, Narayanan emphasizes that the community of developers and academics behind it is unique. "It's a remarkable body of knowledge, and we're going to be teaching this in computer science classes in 20 years, I'm certain of that." ■

**Andy Extance** *is a freelance writer in Exeter, UK.*


1. Nakamoto, S. *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008); available at https://bitcoin.org/bitcoin.pdf
2. Courtois, N. T., Grajek, M. & Naik, R. Preprint available at http://arxiv.org/abs/1310.7935 (2013).
3. O'Dwyer, K. J. & Malone, D. *25th IET Irish Signals & Systems Conf. 2014 and 2014 China-Ireland Int. Conf. on Information and Communities Technologies* 280–285 (2014).
4. Miller, A., Shi, E., Kosba, A. & Katz, J. *ACM Conf. Computer and Communications Security* (2015); preprint available at http://go.nature.com/2i2sfe
5. Miller, A., Juels, A., Shi, E., Parno, B. & Katz, J. *IEEE Symp. Security and Privacy* 475–490 (2014).
6. Goldfeder, S. *et al. Securing Bitcoin Wallets via a New DSA/ECDSA Threshold Signature Scheme* (2015); available at http://go.nature.com/rnqp4q
7. Courtois, N. T., Emirdag, P. & Valsorda, F. *Cryptology ePrint Archive Report 2014/088* (2014).
8. Juels, A., Kosba, A. & Shi, E. *The Ring of Gyges: Using Smart Contracts for Crime* (2015); Preprint available at http://go.nature.com/sbsdqk