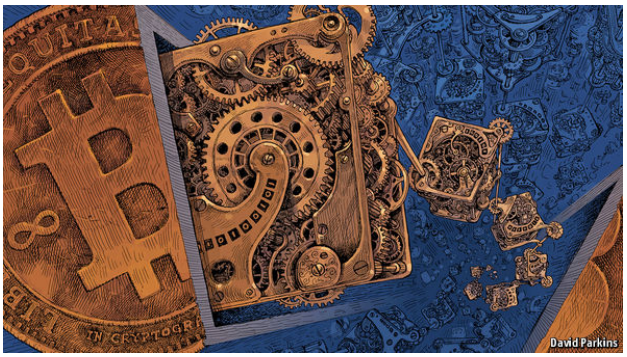
The Economist

Blockchains

The great chain of being sure about things

The technology behind bitcoin lets people who do not know or trust each other build a dependable ledger. This has implications far beyond the cryptocurrency

Oct 31st 2015 | From the print edition



WHEN the Honduran police came to evict her in 2009 Mariana Catalina Izaguirre had lived in her lowly house for three decades. Unlike many of her neighbours in Tegucigalpa, the country's capital, she even had an official title to the land on which it stood. But the records at the country's Property Institute showed another person registered as its owner, too—and that person convinced a judge to sign an eviction order. By the time the legal confusion was finally sorted out, Ms Izaguirre's house had been demolished.

It is the sort of thing that happens every day in places where land registries are badly kept, mismanaged and/or corrupt—which is to say across much of the world. This lack of secure property rights is an endemic source of insecurity and injustice. It also makes it harder to use a house or a piece of land as collateral, stymying investment and job creation.

Such problems seem worlds away from bitcoin, a currency based on clever cryptography which has a devoted following among mostly well-off, often anti-government and sometimes criminal geeks. But the cryptographic technology that underlies bitcoin, called the "blockchain", has applications well beyond cash and currency. It offers a way for people who do not know or trust each other to create a record of who owns what that will compel the assent of everyone concerned. It is a way of making and preserving truths.

That is why politicians seeking to clean up the Property Institute in Honduras have asked Factom, an American startup, to provide a prototype of a blockchain-based land registry. Interest in the idea has also been expressed in Greece, which has no proper land registry and where only 7% of the territory is adequately mapped.

A place in the past

Other applications for blockchain and similar "distributed ledgers" range from thwarting diamond thieves to streamlining stockmarkets: the NASDAQ exchange will soon start using a blockchain-based system to record trades in privately held companies. The Bank of England, not known for technological flights of fancy, seems electrified: distributed ledgers, it concluded in a research note late last year, are a "significant innovation" that could have "far-reaching implications" in the financial industry.

The politically minded see the blockchain reaching further than that. When co-operatives and left-wingers gathered for this year's OuiShare Fest in Paris to discuss ways that grass-roots organisations could undermine giant repositories of data like Facebook, the blockchain made it into almost every speech. Libertarians dream of a world where more and more state regulations are replaced with private contracts between individuals—contracts which blockchain-based programming would make self-enforcing.

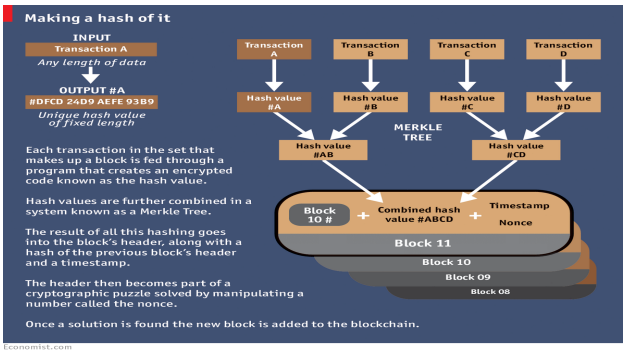
The blockchain began life in the mind of Satoshi Nakamoto, the brilliant, pseudonymous and so far unidentified creator of bitcoin—a "purely peer-to-peer version of electronic cash", as he put it in a paper published in 2008. To work as cash, bitcoin had to be able to change hands without being diverted into the wrong account and to be incapable of being spent twice by the same person. To fulfil Mr Nakamoto's dream of a decentralised system the avoidance of such abuses had to be achieved without recourse to any trusted third party, such as the banks which stand behind conventional payment systems.

It is the blockchain that replaces this trusted third party. A database that contains the payment history of every bitcoin in circulation, the blockchain provides proof of who owns what at any given juncture. This distributed ledger is replicated on thousands of computers—bitcoin's "nodes"—around the world and is publicly available. But for all its openness it is also trustworthy and secure. This is guaranteed by the mixture of mathematical subtlety and computational brute force built into its "consensus mechanism"—the process by which the nodes agree on how to update the blockchain in the light of bitcoin transfers from one person to another.

Let us say that Alice wants to pay Bob for services rendered. Both have bitcoin "wallets"—software which accesses the blockchain rather as a browser accesses the web, but does not identify the user to the system. The transaction starts with Alice's wallet proposing that the blockchain be changed so as to show Alice's wallet a little emptier and Bob's a little fuller.

The network goes through a number of steps to confirm this change. As the proposal propagates over the network the various nodes check, by inspecting the ledger, whether Alice actually has the bitcoin she now wants to spend. If everything looks kosher, specialised nodes called miners

will bundle Alice's proposal with other similarly reputable transactions to create a new block for the blockchain.



This entails repeatedly feeding the data through a cryptographic "hash" function which boils the block down into a string of digits of a given length (see diagram). Like a lot of cryptography, this hashing is a one-way street. It is easy to go from the data to their hash; impossible to go from the hash back to the data. But though the hash does not contain the data, it is still unique to them. Change what goes into the block in any way—alter a transaction by a single digit—and the hash would be different.

Running in the shadows

That hash is put, along with some other data, into the header of the proposed block. This header then becomes the basis for an exacting mathematical puzzle which involves using the hash function yet again. This puzzle can only be solved by trial and error. Across the network, miners grind through trillions and trillions of possibilities looking for the answer. When a miner finally comes up with a solution other nodes quickly check it (that's the one-way street again: solving is hard but checking is easy), and each node that confirms the solution updates the blockchain accordingly. The hash of the header becomes the new block's identifying string, and that block is now part of the ledger. Alice's payment to Bob, and all the other transactions the block contains, are confirmed.

This puzzle stage introduces three things that add hugely to bitcoin's security. One is chance. You cannot predict which miner will solve a puzzle, and so you cannot predict who will get to update the blockchain at any given time, except in so far as it has to be one of the hard working miners, not some random interloper. This makes cheating hard.

The second addition is history. Each new header contains a hash of the previous block's header, which in turn contains a hash of the header before that, and so on and so on all the way back to the beginning. It is this concatenation that makes the blocks into a chain. Starting from all the data in the ledger it is trivial to reproduce the header for the latest block. Make a change anywhere, though—even back in one of the earliest blocks—and that changed block's header will come out different. This means that so will the next block's, and all the subsequent ones. The ledger will no longer match the latest block's identifier, and will be rejected.

Is there a way round this? Imagine that Alice changes her mind about paying Bob and tries to

rewrite history so that her bitcoin stays in her wallet. If she were a competent miner she could solve the requisite puzzle and produce a new version of the blockchain. But in the time it took her to do so, the rest of the network would have lengthened the original blockchain. And nodes always work on the longest version of the blockchain there is. This rule stops the occasions when two miners find the solution almost simultaneously from causing anything more than a temporary fork in the chain. It also stops cheating. To force the system to accept her new version Alice would need to lengthen it faster than the rest of the system was lengthening the original. Short of controlling more than half the computers—known in the jargon as a "51% attack"—that should not be possible.

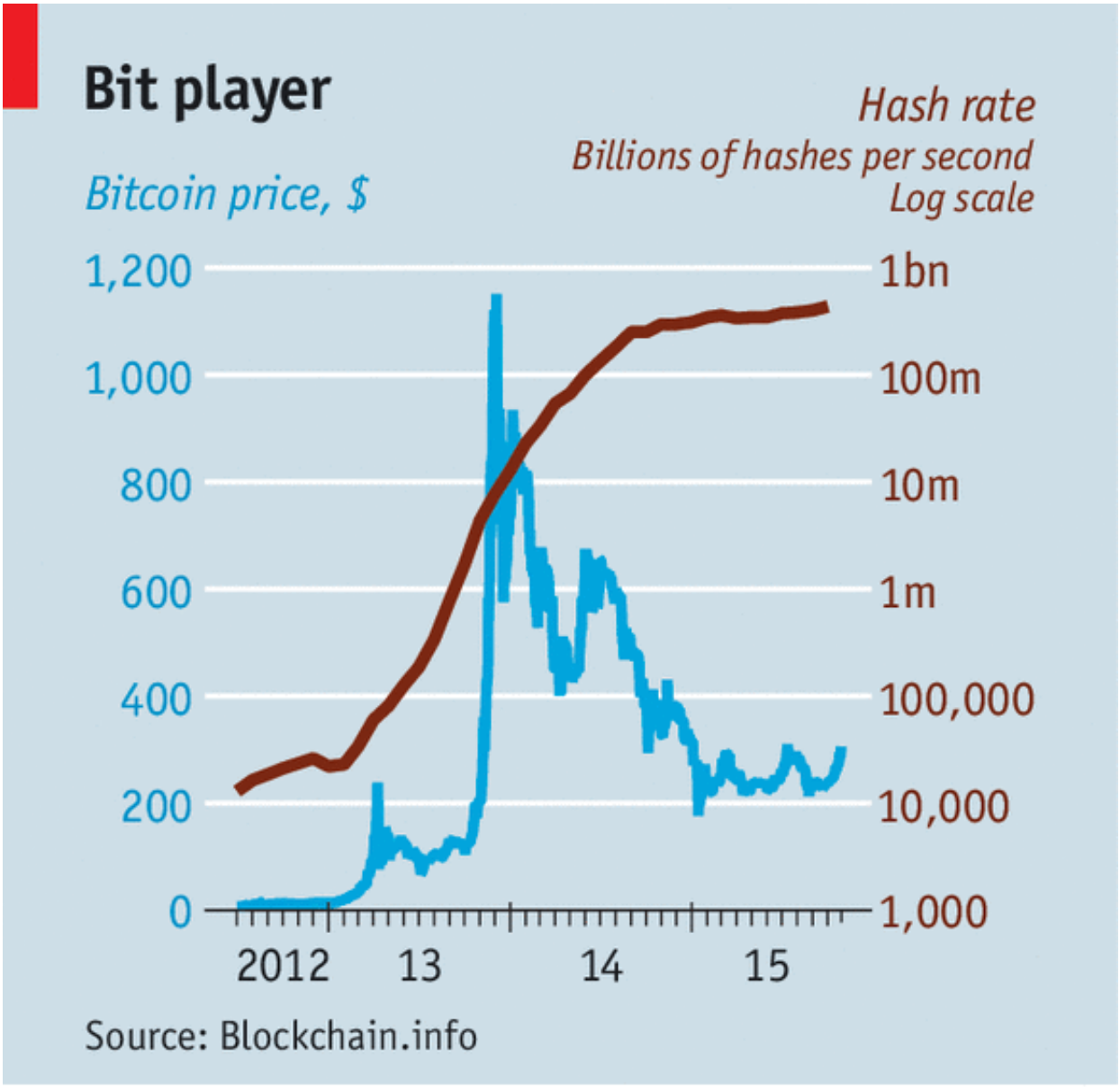
Dreams are sometimes catching

Leaving aside the difficulties of trying to subvert the network, there is a deeper question: why bother to be part of it at all? Because the third thing the puzzle-solving step adds is an incentive. Forging a new block creates new bitcoin. The winning miner earns 25 bitcoin, worth about $7,500 at current prices.

All this cleverness does not, in itself, make bitcoin a particularly attractive currency. Its value is unstable and unpredictable (see chart), and the total amount in circulation is deliberately limited. But the blockchain mechanism works very well. According to blockchain.info, a website that tracks such things, on an average day more than 120,000 transactions are added to the blockchain, representing about $75m exchanged. There are now 380,000 blocks; the ledger weighs in at nearly 45 gigabytes.

Most of the data in the blockchain are about bitcoin. But they do not have to be. Mr Nakamoto has built what geeks call an "open platform"—a distributed system the workings of which are open to examination and elaboration. The paragon of such platforms is the internet itself; other examples include operating systems like Android or Windows. Applications that depend on basic features of the blockchain can thus be developed without asking anybody for permission or paying anyone for the privilege. "The internet finally has a public data base," says Chris Dixon of Andreessen Horowitz, a venture-capital firm which has financed several bitcoin start-ups, including Coinbase, which provides wallets, and 21, which makes bitcoin-mining hardware for the masses.

For now blockchain-based offerings fall in three buckets. The first takes advantage of the fact that any type of asset can be transferred using the blockchain. One of the startups betting on this idea is Colu. It has developed a mechanism to "dye" very small bitcoin transactions (called "bitcoin dust") by adding extra data to them so that they can represent bonds, shares or units of precious metals.



Economist.com

Protecting land titles is an example of the second bucket: applications that use the blockchain as a truth machine. Bitcoin transactions can be combined with snippets of additional information which then also become embedded in the ledger. It can thus be a registry of anything worth tracking closely. Everledger uses the blockchain to protect luxury goods; for example it will stick on to the blockchain data about a stone's distinguishing attributes, providing unchallengeable proof of its identity should it be stolen. Onename stores personal information in a way that is meant to do away with the need for passwords; CoinSpark acts as a notary. Note, though, that for these applications, unlike for pure bitcoin transactions, a certain amount of trust is required; you have to believe the intermediary will store the data accurately.

It is the third bucket that contains the most ambitious applications: "smart contracts" that execute themselves automatically under the right circumstances. Bitcoin can be "programmed" so that it only becomes available under certain conditions. One use of this ability is to defer the

payment miners get for solving a puzzle until 99 more blocks have been added—which provides another incentive to keep the blockchain in good shape.

Lighthouse, a project started by Mike Hearn, one of bitcoin's leading programmers, is a decentralised crowdfunding service that uses these principles. If enough money is pledged to a project it all goes through; if the target is never reached, none does. Mr Hearn says his scheme will both be cheaper than non-bitcoin competitors and also more independent, as governments will be unable to pull the plug on a project they don't like.

Energy is contagious

The advent of distributed ledgers opens up an "entirely new quadrant of possibilities", in the words of Albert Wenger of USV, a New York venture firm that has invested in startups such as OpenBazaar, a middleman-free peer-to-peer marketplace. But for all that the blockchain is open and exciting, sceptics argue that its security may yet be fallible and its procedures may not scale. What works for bitcoin and a few niche applications may be unable to support thousands of different services with millions of users.

Though Mr Nakamoto's subtle design has so far proved impregnable, academic researchers have identified tactics that might allow a sneaky and well financed miner to compromise the block chain without direct control of 51% of it. And getting control of an appreciable fraction of the network's resources looks less unlikely than it used to. Once the purview of hobbyists, bitcoin mining is now dominated by large "pools", in which small miners share their efforts and rewards, and the operators of big data centres, many based in areas of China, such as Inner Mongolia, where electricity is cheap.

Another worry is the impact on the environment. With no other way to establish the bona fides of miners, the bitcoin architecture forces them to do a lot of hard computing; this "proof of work", without which there can be no reward, insures that all concerned have skin in the game. But it adds up to a lot of otherwise pointless computing. According to blockchain.info the network's miners are now trying 450 thousand trillion solutions per second. And every calculation takes energy.

Because miners keep details of their hardware secret, nobody really knows how much power the network consumes. If everyone were using the most efficient hardware, its annual electricity usage might be about two terawatt-hours—a bit more than the amount used by the 150,000 inhabitants of King's County in California's Central Valley. Make really pessimistic assumptions about the miners' efficiency, though, and you can get the figure up to 40 terawatt-hours, almost two-thirds of what the 10m people in Los Angeles County get through. That surely overstates the problem; still, the more widely people use bitcoin, the worse the waste could get.

Yet for all this profligacy bitcoin remains limited. Because Mr Nakamoto decided to cap the size of a block at one megabyte, or about 1,400 transactions, it can handle only around seven transactions per second, compared to the 1,736 a second Visa handles in America. Blocks could be made bigger; but bigger blocks would take longer to propagate through the network, worsening the risks of forking.

Earlier platforms have surmounted similar problems. When millions went online after the invention of the web browser in the 1990s pundits predicted the internet would grind to a standstill: *eppur si muove*. Similarly, the bitcoin system is not standing still. Specialised mining computers can be very energy efficient, and less energy-hungry alternatives to the proof-of-work mechanism have been proposed. Developers are also working on an add-on called "Lightning" which would handle large numbers of smaller transactions outside the blockchain. Faster connections will let bigger blocks propagate as quickly as small ones used to.

The problem is not so much a lack of fixes. It is that the network's "bitcoin improvement process" makes it hard to choose one. Change requires community-wide agreement, and these are not people to whom consensus comes easily. Consider the civil war being waged over the size of blocks. One camp frets that quickly increasing the block size will lead to further concentration in the mining industry and turn bitcoin into more of a conventional payment processor. The other side argues that the system could crash as early as next year if nothing is done, with transactions taking hours.

A break in the battle

Mr Hearn and Gavin Andresen, another bitcoin grandee, are leaders of the big-block camp. They have called on mining firms to install a new version of bitcoin which supports a much bigger block size. Some miners who do, though, appear to be suffering cyber-attacks. And in what seems a concerted effort to show the need for, or the dangers of, such an upgrade, the system is being driven to its limits by vast numbers of tiny transactions.

This has all given new momentum to efforts to build an alternative to the bitcoin blockchain, one that might be optimised for the storing of distributed ledgers rather than for the running of a cryptocurrency. MultiChain, a build-your-own-blockchain platform offered by Coin Sciences, another startup, demonstrates what is possible. As well as offering the wherewithal to build a public blockchain like bitcoin's, it can also be used to build private chains open only to vetted users. If all the users start off trusted the need for mining and proof-of-work is reduced or eliminated, and a currency attached to the ledger becomes an optional extra.

The first industry to adopt such sons of blockchain may well be the one whose failings originally inspired Mr Nakamoto: finance. In recent months there has been a rush of bankerly enthusiasm

for private blockchains as a way of keeping tamper-proof ledgers. One of the reasons, irony of ironies, is that this technology born of anti-government libertarianism could make it easier for the banks to comply with regulatory requirements on knowing their customers and anti-money-laundering rules. But there is a deeper appeal.

Industrial historians point out that new powers often become available long before the processes that best use them are developed. When electric motors were first developed they were deployed like the big hulking steam engines that came before them. It took decades for manufacturers to see that lots of decentralised electric motors could reorganise every aspect of the way they made things. In its report on digital currencies, the Bank of England sees something similar afoot in the financial sector. Thanks to cheap computing financial firms have digitised their inner workings; but they have not yet changed their organisations to match. Payment systems are mostly still centralised: transfers are cleared through the central bank. When financial firms do business with each other, the hard work of synchronising their internal ledgers can take several days, which ties up capital and increases risk.

Distributed ledgers that settle transactions in minutes or seconds could go a long way to solving such problems and fulfilling the greater promise of digitised banking. They could also save banks a lot of money: according to Santander, a bank, by 2022 such ledgers could cut the industry's bills by up to $20 billion a year. Vendors still need to prove that they could deal with the far-higher-than-bitcoin transaction rates that would be involved; but big banks are already pushing for standards to shape the emerging technology. One of them, UBS, has proposed the creation of a standard "settlement coin". The first order of business for R3 CEV, a blockchain startup in which UBS has invested alongside Goldman Sachs, JPMorgan and 22 other banks, is to develop a standardised architecture for private ledgers.

The banks' problems are not unique. All sorts of companies and public bodies suffer from hard-to-maintain and often incompatible databases and the high transaction costs of getting them to talk to each other. This is the problem Ethereum, arguably the most ambitious distributed-ledger project, wants to solve. The brainchild of Vitalik Buterin, a 21-year-old Canadian programming prodigy, Ethereum's distributed ledger can deal with more data than bitcoin's can. And it comes with a programming language that allows users to write more sophisticated smart contracts, thus creating invoices that pay themselves when a shipment arrives or share certificates which automatically send their owners dividends if profits reach a certain level. Such cleverness, Mr Buterin hopes, will allow the formation of "decentralised autonomous organisations"—virtual companies that are basically just sets of rules running on Ethereum's blockchain.

One of the areas where such ideas could have radical effects is in the "internet of things"—a

network of billions of previously mute everyday objects such as fridges, doorstops and lawn sprinklers. A recent report from IBM entitled "Device Democracy" argues that it would be impossible to keep track of and manage these billions of devices centrally, and unwise to to try; such attempts would make them vulnerable to hacking attacks and government surveillance. Distributed registers seem a good alternative.

The sort of programmability Ethereum offers does not just allow people's property to be tracked and registered. It allows it to be used in new sorts of ways. Thus a car-key embedded in the Ethereum blockchain could be sold or rented out in all manner of rule-based ways, enabling new peer-to-peer schemes for renting or sharing cars. Further out, some talk of using the technology to make by-then-self-driving cars self-owning, to boot. Such vehicles could stash away some of the digital money they make from renting out their keys to pay for fuel, repairs and parking spaces, all according to preprogrammed rules.

What would Rousseau have said?

Unsurprisingly, some think such schemes overly ambitious. Ethereum's first ("genesis") block was only mined in August and, though there is a little ecosystem of start-ups clustered around it, Mr Buterin admitted in a recent blog post that it is somewhat short of cash. But the details of which particular blockchains end up flourishing matter much less than the broad enthusiasm for distributed ledgers that is leading both start-ups and giant incumbents to examine their potential. Despite society's inexhaustible ability to laugh at accountants, the workings of ledgers really do matter.

Today's world is deeply dependent on double-entry book-keeping. Its standardised system of recording debits and credits is central to any attempt to understand a company's financial position. Whether modern capitalism absolutely required such book-keeping in order to develop, as Werner Sombart, a German sociologist, claimed in the early 20th century, is open to question. Though the system began among the merchants of renaissance Italy, which offers an interesting coincidence of timing, it spread round the world much more slowly than capitalism did, becoming widely used only in the late 19th century. But there is no question that the technique is of fundamental importance not just as a record of what a company does, but as a way of defining what one can be.

Ledgers that no longer need to be maintained by a company—or a government—may in time spur new changes in how companies and governments work, in what is expected of them and in

what can be done without them. A realisation that systems without centralised record-keeping can be just as trustworthy as those that have them may bring radical change.

Such ideas can expect some eye-rolling—blockchains are still a novelty applicable only in a few niches, and the doubts as to how far they can spread and scale up may prove well founded. They can also expect resistance. Some of bitcoin's critics have always seen it as the latest techy attempt to spread a "Californian ideology" which promises salvation through technology-induced decentralisation while ignoring and obfuscating the realities of power—and happily concentrating vast wealth in the hands of an elite. The idea of making trust a matter of coding, rather than of democratic politics, legitimacy and accountability, is not necessarily an appealing or empowering one.

At the same time, a world with record-keeping mathematically immune to manipulation would have many benefits. Evicted Ms Izaguirre would be better off; so would many others in many other settings. If blockchains have a fundamental paradox, it is this: by offering a way of setting the past and present in cryptographic stone, they could make the future a very different place.

From the print edition: Briefing