The Coming Digital REVOLUTION

Bitcoin is giving banks a run for their money. Now the same technology threatens to eradicate social networks, stock markets, even national governments. Are we heading towards an anarchic future where centralised power of any kind will dissolve?

The same technology that powers Bitcoin can be harnessed to disrupt a range of other systems Photo: Bloomberg News

The rise and rise of Bitcoin has grabbed the world's attention, yet its devastating potential still isn't widely understood. Yes, we all know it's a digital currency. But the developers who worked on Bitcoin believe that it represents a technological breakthrough that could sweep into obsolescence everything from social networks to stock markets... and even governments.

In short, Bitcoin could be the gateway to a coming digital anarchy – "a catalyst for change that creates a new and different world," to quote Jeff Garzik, one of Bitcoin's most prolific developers.

It's already beginning. We used to need banks to keep track of who owned what. Not any more. Bitcoin and its rivals have proved that banks can be replaced with software and clever mathematics.

And now programmers of a libertarian bent are starting to ask what else we don't need.

A Bitcoin dispensing machine at a shopping mall in Singapore

Imagine driverless taxis roaming from city to city in search of the most lucrative fares; a sky dark with hovering drones delivering your shopping or illicit drugs. Digital anarchy could fill your lives and your nightmares with machines that answer to you, your employers, crime syndicates… or no one at all. Nearly every aspect of our lives will be uprooted.

To understand how, we need to grasp the power of the "blockchain" – a peer-to-peer ledger which creates and records agreement on contentious issues with the aid of cryptography.

A blockchain forms the beating heart of Bitcoin. In time, blockchains will power many radical, disruptive technologies that smart people are working on right now.

Until recently, we've needed central bodies – banks, stock markets, governments, police forces – to settle vital questions. Who owns this money? Who controls this company? Who has the right to vote in this election?

Now we have a small piece of pure, incorruptible mathematics enshrined in computer code that will allow people to solve the thorniest problems without reference to "the authorities".

The benefits of decentralised systems will be huge: slashed overheads, improved security and (in many circumstances) the removal of the weakest link of all – greedy, corruptible, fallible humans.

But how far will disruptive effects reach? Are we rapidly approaching a singularity where, thanks to Bitcoin-like tools, centralised power of any kind will seem as archaic as the feudal system?

If the internet revolution has taught us anything, it's that when change comes, it comes fast.

Funny money:

Let's start with digital currency. Right now, in the wake of an unprecedented financial crisis, it's easy to understand the appeal of a new money that lies beyond the grasp of banks and governments.

No treasury can print more Bitcoins and inflate away the value of your savings, or recklessly lend them out for years to people with no chance of meeting repayments, eventually bringing the whole system crashing down. The rules of Bitcoin are set in digital stone.

It all began with a paper written by someone calling himself "Satoshi Nakamoto" and quietly published via a cryptography mailing list in 2008. It laid out a plan for a form of money based on "cryptographic proof instead of trust".

Nakamoto described a way of keeping a ledger of all transactions – the blockchain – to prove who owned what. It was a breakthrough which solved a longstanding computer science problem: how to run a complex system with no central control.

Bitcoin has no bank to maintain security, record ownership or handle transactions. None is needed.

The true identity of Satoshi has never been revealed, although rumours abound: a lone academic, a group of disgruntled, anarchist programmers working in the financial sector, the CIA...

What is known is that the number of coins in circulation is finite, limited to 21 million. The plan is immutable: around 13 million are already in existence and the last ones will be released in 20 years or so.

Critics who say Bitcoin is nothing but zeros and ones in a computer file and therefore can't hold value miss the point that their bank balance is, similarly, nothing but a number on a computer.

The pound is worth something only because people decide to place value in it. If that consensus broke down, then – as in Weimar Germany – a wheelbarrow full of £20 notes couldn't buy you a cup of coffee. Sterling is a famously stable currency – but just occasionally we're brought up with a jolt. For example, in 2007 Northern Rock was forced to go cap-in-hand to the Bank of England. A few customers rushed to withdraw their money, then a few more... and soon there was panic. Loss of faith. Shades of Weimar, or even Zimbabwe.

If national currencies can fall victim to a chain-reaction erosion of faith, why should a new currency not experience the same phenomenon in reverse?

Last year Cyprus horrified citizens when it announced that it would seize up to 60 per cent of all savings over €100,000 to save its struggling banks. Suddenly Bitcoin seemed less risky and transaction volumes soared as people poured cash into the digital currency to keep it out of government coffers.

Protests in Nicosia, Cyprus, in 2013 against a tax on bank deposits (BLOOMBERG)

This same land grab could not happen with Bitcoin. There is no central power with the ability to skim off the top.

Neither are credit-fuelled binges possible. The smoke-and-mirrors system that banks use to magic money into existence when they create loans is not possible in a Bitcoin world.

This holds a lot of appeal. Financial Times columnist Martin Wolf recently called for banks to be stripped of this bizarre right to create money from thin air, claiming that it was the root cause of credit bubbles and busts such as the painful cycle we have just witnessed. In his view, they should be confined to only lending the amount they have taken as deposits from savers. It's hard to argue against such a commonsense proposal.

It is perhaps no coincidence that Bitcoin emerged from the ashes of a savage recession. Although it is radical in many ways, it is also strictly conservative: no debt is possible, no complex derivatives, no untrustworthy middlemen. You either have coins, or you don't.

The timing was impeccable, the perfect antidote to a financial system which can't be trusted not to lead us into another round of boom and bust.

The old order: controlling the internet

The banks aren't the only institutions whose future is threatened. The blockchain has the power to uproot a number of our most recognisable dot coms.

The internet, rife with accidental data leaks like eBay's latest mishap and government eavesdropping, is crying out for anarchic disruption. Lack of trust in banks has become lack of trust in the guardians of cyberspace. There is a growing mood that nobody can be trusted with our money or our data.

We think of the internet as a libertarian free-for-all, a place where anything goes and governments fear to tread. But nothing could be further from the truth. The Internet was a US invention born out of the Department of Defence in the late 60s, and the American government keeps a firm grip on the reins to this day.

In the 90s maintenance of the internet was overseen by just one man: a computer scientist, on the payroll of the Department, called Jon Postel. Once the job outgrew him, the US government set up a nonprofit called the Internet Corporation for Assigned Names and Numbers (ICANN) to take over the task. It now keeps track of who owns which domain names and maintains various systems that underpin the internet and the World Wide Web.

ICANN presents itself as a friendly caretaker and security guard, with an altruistic motto: "One World. One Internet." It operates under a mandate from the US government to run things in a "bottom up, consensus driven, democratic manner". Its blog – yes, it has a blog – switches fluently from Silicon Valley gush ("this incredible journey") to corporate jargon ("a multistakeholder approach to the future evolution of Internet governance").

Since 2010, ICANN has opened four new offices – in Los Angeles, Washington DC, Brussels and (of course) Silicon Valley. As its website boasts: "The contemporary architecture of all four offices visually expresses ICANN's organisational mandate for transparency through glass office and conference room walls and floor-to-ceiling windows that allow in natural light."

But does ICANN's operational transparency match that of its gleaming windows?

Its advisory committee of national governments, the World Bank, the World Trade Organisation and Interpol is often criticised for deciding important matters behind closed doors. And the most recent moves towards "transparency" seem designed to achieve the opposite. ICANN wants to restrict access to Whois, a facility that allows anyone to know who has registered a domain name on the internet. Instead, this information would be available to "appropriate" interested parties.

Put bluntly, the global machinery of the internet is operated by a conglomerate dominated by governments – and especially the US government.

Also, individual governments around the world have their own censorship tools. The crucial point is that censorship is a spectrum. Few of us would object to the UK's practice of blocking child pornography – but what about the banning of file-sharing websites? Or the ham-fisted blocking of any information critical of an authoritarian regime?

Meanwhile, largely thanks to Edward Snowden, we're waking up to the fact that the same governments which restrict what we can see are themselves able to peer into our private lives.

GCHQ Headquarters in Cheltenham

Documents leaked by Snowden revealed that the UK's hi-tech spy agency GCHQ, based in Cheltenham, has captured images from private webcam conversations between people of no interest in any ongoing investigation – "unselected", in their slightly chilling terminology.

Over a million webcam users were caught up in this fishing expedition. Many of these images turned out to be sexually explicit. They remain on file in Cheltenham.

The new order: unravelling the internet

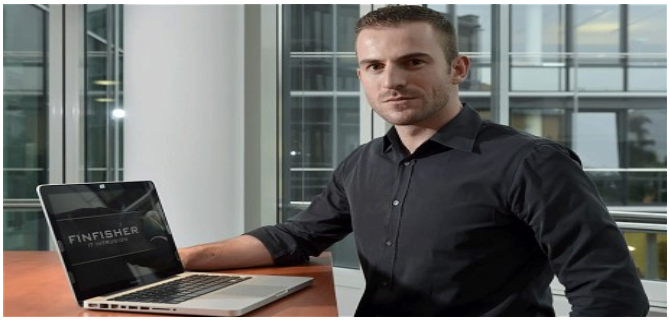
America and Britain have the resources to create tools to pull off tricks like these themselves. Smaller countries turn to the private sector, which is only too delighted to help out. And this is where the game changes: from controlling the internet to unravelling it.

Andover is a mildly picturesque market town in Hampshire. It's an unlikely setting for the offices of Gamma, a controversial internet security company that sells FinFisher, described by Bloomberg as "one of the world's most elusive cyberweapons, which can secretly take remote control of a computer, copying files, intercepting Skype calls and logging every keystroke".

In the aftermath of the Arab Spring, the BBC reported that it had seen documents in the looted headquarters of the Egyptian state security building that suggested Gamma software had been used in a five-month trial to target pro-democracy activists. The company denied supplying the software. (It failed to respond to requests for comment when the Telegraph contacted it.)

Gamma's managing director, Martin Muench, is in his early 30s, dresses in black and comes from a small town in north Germany that he won't name because he fears for his family's security. He says FinFisher helps captures paedophiles and terrorists, who regard him as "the personified evil".

He's not popular among human rights activists in Bahrain, either: as Bloomberg reported in detail, they claim FinFisher has been used against them. Muench denies that FinFisher is a tool for tyrants. He's someone who carefully guards his reputation and his privacy. If you look closely at the photograph Bloomberg took of him standing next to his Apple laptop, you'll see that he seems to have a small sticker covering its webcam lens.



Gamma's managing director, Martin Muench (BLOOMBERG)

Muench and Gamma operate within the law: FinFisher is not an illegal tool, though it can be used illegally.

Tweak the technology a bit, however, and you have something like Blackshades Remote Access Tool (RAT), which is regarded as "malicious commercial software".

Blackshades RAT was used last year to capture naked photographs of the then 19-year-old Miss Teen USA Cassidy Wolf. Jared James Abrahams, 20, threatened to post the photos online unless Wolf gave him a nude video. He was later sentenced to 18 months in prison.

At the end of May this year, nearly 100 people were arrested in a worldwide crackdown on the creators, sellers and users of Blackshades RAT. It's a hackers' and blackmailers' tool. Follow its trail and you'll soon find yourself in strange places. Police making the Blackshade arrests seized 1,100 data storage devices suspected of being used in illegal activities. They also found stolen cash, guns and drugs.

Organised crime is technology-obsessed. That makes life tough for law enforcement – but it's also evidence of a wider trend.

Governments and agencies companies which have, until now, had total control over the internet are fast losing it. Like holding a handful of sand: the harder they squeeze, the quicker it slips away.

Here's an illustration. The University of Abertay in Dundee now offers a four-year BSc in "Ethical Hacking". Abertay is a minor university and some of its other courses – eg, a BSc in "Performance Golf" – invite ridicule. So, on the face of it, does "Ethical Hacking", which could mean anything.

Click through to details of the course, however, and you realise that it's cleverly designed to address the growing anxieties of large organisations that live in fear of digital sabotage.

According to the prospectus, "the business world is seeing a rapid increase in the demand for ethical or white hat, hackers, employed by companies to find security holes before criminal, black hat, hackers do … Hackers are innately curious and want to pull things apart. They experiment and research. A hacker wants to learn and investigate. The aim is for you to arrive on this programme as a student and leave as an ethical hacker."

Graduates will have state-of-the-art knowledge of penetration testing, cryptography and biometric identity systems. They will be intimately familiar with the habits of "black hat" hackers.

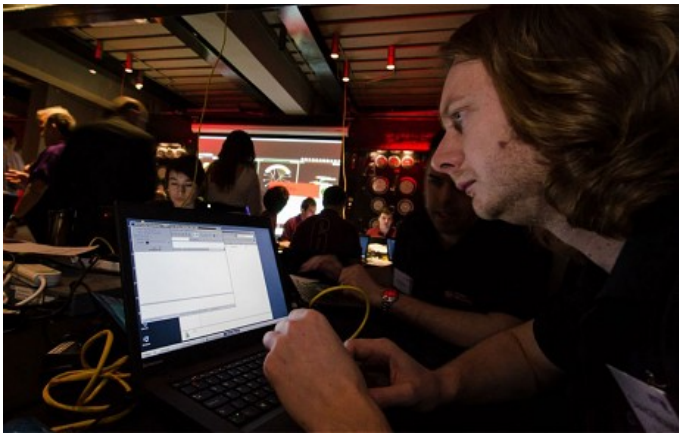
As a result, they will not find it difficult to land well-paid jobs. Many of these jobs could even be inside GCHQ itself.

The agency sponsors an annual hacking tournament which attracts thousands of entrants of exactly the kind that The University of Abertay is after, who are whittled down through numerous online rounds to the few dozen who take part in a final and extremely realistic cyber-attack simulation. This year it was **held in the Cabinet War Rooms deep beneath Whitehall**.

At this year's event I spoke to a man from Cheltenham who refused to give me his name, who said that "some of the skills you see here today are what GCHQ would be doing". He was one of many people watching proceedings wearing a special armband whom I was forbidden from photographing.

Later, I asked Stephanie Daman, chief executive of the Cyber Security Challenge, how many of the people in the room would be hoovered up by the security agencies, but was told with a smile that such things aren't revealed.

But if somebody performed well and then didn't reappear next year? You can make your own inferences from that, she said: "We're not a recruitment agency. We provide a place for people to meet."



The Cyber Security Challenge, held in London (MATTHEW SPARKES)

Whether these ethical hackers will stay ethical is another question, however.

Social networks, search engines and online retailers have grown rich by soaking up our personal data and distilling it into valuable databases used to surgically target advertising.

As the adage goes: "If you're not paying, then you're the product". You don't pay a penny for Google's search engine, email or calendar products. What you do provide, though, is data on every aspect of your life: who you know; where you go; what you enjoy eating, wearing, watching.

An unimaginable amount of information is being analysed and exploited by companies in order to screw money out of us. But rather than having to collect it, we are handing it to them in return for a simple, free way to chat to our friends, share pictures or send emails.

Behind the laid-back, let's-play-table-football facade of Silicon Valley firms lies a sneakiness and paranoia that, critics say, verges on the sociopathic. This is hardly surprising. The giant dotcoms stand to lose billions of dollars and even kick-start a US recession if the internet becomes too unstable for them to manage. But, in addition, they need to take advantage of digital instability in order to shaft their rivals.

"These guys are control freaks who see themselves as 'disruptive', to quote one of their favourite words," says a California-based analyst. "It's a very combustible mixture particularly when you consider the endless, endless uncertainty they face every day."

The biggest corporations work overtime to maintain the appearance of omnipotence. Dave Eggers satirises one such firm in his novel The Circle, about a sinister West Coast dotcom whose slogans include "secrets are lies" and "privacy is theft".

In an interview with McSweeneys, Eggers said he often had to delete sections of his manuscript when truth caught up with fiction: "A lot of times I'd think of something that a company like the Circle might dream up, something a little creepy, and then I'd read about the exact invention, or even something more extreme, the next day."

Now we need to put our finger on a really important paradox that lies at the heart of the coming digital anarchy.

The hidden power of the Facebooks, Twitters and Googles of this world is inspiring digital anarchists to destroy the smug, jargon-infested giants of Silicon Valley. But who are these hackers? They're unlikely to be career criminals who identify themselves by their black hats. On the contrary, they may well have picked up their techniques while working in Palo Alto.

In some cases, the very same people who helped create these mega-corporations are now working on "disruptive technologies" to replace them.

We think of Silicon Valley as peopled by "liberals". But that's misleading. They may be socially liberal, but their "libertarianism" is often predicated on very low taxes funding a very small government. They have a soft spot for the anti-tax Republican Rand Paul and the kill-or-be-killed ethos of the paranoid libertarian capitalist Ayn Rand (whom Mr Paul was not named after, though he's had to spend his whole life denying it).

The digital utopias at the back of these

people’s minds are often startlingly weird.

Consider, for example, Peter Thiel, the founder of PayPal – ironically, one of the companies Bitcoin aims to blow out of the water. He has donated $1.25m to the SeaSteading Institute, a group which aims to create an autonomous nation in the ocean, away from existing sovereign laws and free of regulation.

At a conference in 2009 he said: "There are quite a lot of people who think it's not possible. That's a good thing. We don't need to really worry about those people very much, because since they don't think it's possible they won't take us very seriously. And they will not actually try to stop us until it's too late."

It’s difficult to generalise about motives when the membranes separating control and anarchy, creativity and disruption, greed and philanthropy have become so alarmingly thin. Remember that the entrepreneurs of Silicon Valley and its many global franchises are usually young enough to be impressionable and excitable. Yes, some of them they may qualify as utopians – but, like utopians throughout history, they are ready to use destructive tactics to reach their goal.

What is that goal? Right now, and put simply, it’s to create what they regard as “incorruptible” versions of the websites, networks and financial institutions which we all rely on every day – to remove the man in the middle and any ulterior motives he may have.

The new digital anarchists – who are as likely to wear Gant chinos as hoodies, and wouldn’t be seen dead in an Anonymous mask – are in the mood to punish Facebook, Google, Twitter, PayPal, eBay, you name it, for their arrogance. Indeed, they may have encountered this arrogance close up by working for them. That’s enough of a motive for the great digital unravelling.

As for means and opportunity – well, they now have their weapon of choice: the blockchain.

We need to understand more about this concept, so let’s return to Bitcoin and peer beneath the bonnet.

Why the blockchain changes everything

In our current banking system we all have accounts holding certain amounts of money. To pay for a coffee at Starbucks we tell the bank, often via a chip-and-PIN machine, that we’d like to transfer £3. Starbucks’s account balance goes up £3, ours goes down £3, and the bank tallies the books.

Bitcoin removes the banker, the man in the middle, who can choose to levy fees, disclose information to governments... or do anything else they see fit which may anger your average libertarian anarchist. (Some of them live in a permanent state of resentment, it should be said.)

But doing so is far from simple. Who tracks how much money everyone has, if not the bank? If it were left to individuals, we would all add a few zeros to our balances and the whole thing would descend into a fraudulent farce.

Bitcoin’s solution is for everyone to record all information. We will all be the bank. As we saw earlier, the blockchain is the public ledger of all transactions, showing how much each person owns, and it is stored by Bitcoin users all over the planet.

The clever part is how the network reaches a consensus on what should be written in it. Otherwise there could be thousands of different blockchains, all disagreeing over who owns what.

The idea is that each and every transaction is broadcast by the person initiating it. Rather than telling the bank we want to spend £3, we tell the world. That transaction is bundled up with thousands of others and cryptographically bound into a “block” by “miners”.

Technically, anyone with a computer can be a miner – they just need to install a small piece of software. But it’s not easy to do: far from it.

Bitcoin “miners” are so called because gold miners traditionally have to put in a lot of work

before they see any reward in the shape of precious metal. In the world of Bitcoin, miners have to crack an extremely difficult cryptographic problem before they are rewarded with some newly minted Bitcoins. That "block" is then added to the end of the blockchain and shared around the world.

To quote the wiki dictionary maintained by "the Bitcoin community" – perhaps the nearest you can get to an official explanation – "mining is intentionally designed to be resource-intensive and difficult so that the number of blocks found each day by miners remains steady … The primary purpose of mining is to allow Bitcoin nodes to reach a secure, tamper-resistant consensus."

In other words, the blockchain remains both public and infallible. It's a totally reliable and trustworthy record of who owns what, but also who owned what back through time, all the way to the creation of Bitcoin.

Anyone attempting to alter that ledger to steal a coin would have to re-do all of the difficult calculations that were done to embed it there the last time it was traded. Then they would have to do the same with all the later blocks on top of it up to the current date, and then get far enough ahead that they were the first people to crack the newest block and get it accepted as the definitive version.

In short, it's impossible.

Our first taste of this decentralised power happened to be a currency, Bitcoin, but it could equally have been a stock exchange, a social network or an electronic voting system.

Jeff Garzik, the Bitcoin developer, tells me that the blockchain technology is "the biggest thing since the internet – a catalyst for change in all areas of our lives".

He's currently fundraising to put Bitcoin satellites into space to rebroadcast the latest version of the blockchain around the world for those without reliable internet connections. That's how strongly he believes in it.

"Currency is simply the first application of Bitcoin's decentralised technology," he tells me from his Atlanta home. "Bitcoin is many layers of an onion. Peel back one layer, and a new and amazing layer awaits underneath to discover."

When power is concentrated in the hands of a few powerful people there is a risk of catastrophe, corruption and chaos, he warns. Decentralising a system hands power to immutable mathematics.

And then the game really changes.

Things fall apart

Remember those luxurious glass offices built by ICANN in order to emphasise its "transparency"? These days an awful lot of anxiety is flooding in along with the sunlight.

ICANN's vice-like grip on domain names is now looking more tenuous than ever before. Currently the group decides which top-level domains can exist (.co.uk for example) and hands out a licence to sell addresses underneath them (such as telegraph.co.uk) to commercial registrars. You pay an annual fee to "own" a domain name.

ICANN then runs a system called DNS which maps these easily remembered domain names to the IP addresses where websites actually reside. Unless your users are willing to remember a long string of numbers such as 93.184.216.119, you have to buy into the domain name system.

Until Namecoin.

This crypto-currency is based on Bitcoin, but instead of acting like money it acts like internet addresses. It has claimed the .bit domain as its own and anybody with Namecoin can use it to reserve an address.

And once you have it, it cannot be taken away: nobody can charge you an annual fee. Suddenly, a small part of ICANN's monopoly could disappear. For the first time, there is a viable alternative.

Now let's make a leap of imagination. It turns out that whole companies are also vulnerable

to being replaced by Bitcoin offshoots.

A project called Twister is attempting to replace Twitter with a peer-to-peer tool based on the blockchain, with messages instead of coins. Unlike Twitter, there is no central company to subpoena or coerce into handing out details of users. If you're an activist in the Middle East posting messages critical of the government, you may feel safer on Twister than Twitter.

Bitmessage aims to do the same thing for email. It's entirely safe, secure and anonymous, with no central point for storage for snooping agencies to target. Downloads of the program increased fivefold during June 2013 after news of email surveillance by the NSA emerged. Companies like Google, Yahoo! and Microsoft which offer webmail should be very worried indeed that there is a free, secure system on the horizon. And they are.

Not all of these replacement systems would be open-source and free. Some could run on the blockchain technology but still make people rich.

Venture capitalist Fred Wilson, who spotted firms such as Twitter, Tumblr and Foursquare early, recently wrote in a blog post: "Our 2004 fund was built during social. Our 2008 fund was built during social and the emergence of mobile. Our 2012 fund was built during the mobile downturn. And our 2014 fund will be built during the blockchain cycle. I am looking forward to it."

One lucrative area will be file storage. In the last few years we've become accustomed to keeping our files "in the cloud" rather than on our own machines. These services seem so simple: we upload our data and can then summon it at will from anywhere in the world.

But they rely on huge data centres full of powerful servers, and multinational companies are the only ones with the resources to build them. Microsoft offer OneDrive, Apple has iCloud and there are others such as Dropbox. All offer a taste for free, but start charging once you pass a certain threshold. Now the Bitcoin protocol threatens this monopoly.

Atlanta-based Shawn Wilkinson is already famous in crypto-currency circles for creating Coingen, a simple service that builds clones of Bitcoin. Want to launch a new currency named after yourself? For just a few pounds Shawn can make it happen.

Now he's launching an online data storage service called Storj that will sit atop the Bitcoin network. Thanks to the thousands of miners, the currency is the largest computing network in the world, says Wilkinson. "Why just use that for money? We want to take the Bitcoin model and apply it to other systems."

The idea is that users' files would be hidden inside the blockchain (or pointers to that file, at least, otherwise the blockchain would quickly bloat to ludicrous proportions). An incentive program would reward those who offer up their own computers for the actual bulk of the storage. If you had a few gigabytes spare on your machine you could temporarily donate them to Storj and earn a few fractions of a Bitcoin each month.

This may sound horribly complex, but the user will be oblivious, says Wilkinson: "You don't care about the technical back-end. You just store your files and it works. When you use Dropbox you don't care about the technical part, you just care that it works."

And people would switch in their droves, he claims, as the price would be orders of magnitude lower than the current offerings.

"Were approaching a completely different economic model here. Now that we have these decentralised technologies, now that we've reduced the cost, what can we do with that? Bitcoin is the largest supercomputing network in the world – it outclasses the top 500 supercomputers by several orders of magnitude and has done since last year."

So what of Google, Apple or Amazon in the post-Storj world? Ultimately, physical computers and hard disks will still be needed. Files cannot be stored on clever ideas alone. But the huge companies that once cornered a

market could be reduced to working for Storj in the hope of picking up incentive payments. No longer would there be rich pickings from users' monthly direct debits.

Braver, smarter companies could instead seize the opportunity to use the blockchain to their own end. Expensive business contracts and financial services could be cut out, for example.

But why stop there?

Bitcoin is a decentralised network designed to replace the financial system. Ethereum is a decentralised network designed to replace absolutely anything that can be described in code: business contracts, the legal system or, as some of Ethereum's more evangelical backers believe, entire states.

Primavera De Filippi, a postdoctoral resreacher at CERSA/CNRS/Université Paris II, is one of Europe's most intellectually dazzling experts on digital and civil rights in cyberspace. She's currently at Harvard, exploring the legal challenges of decentralised digital architectures.

Ethereum, she says, is "really sophisticated, and if any of these platforms are going to take off, I believe it's the one.

"It becomes a completely self-sufficient system, impossible to corrupt. It's a disruptive technology, and society will adapt to it, but it will be a slow process."

The other side of the law

So, what if we are on the verge of developing methods of data transformation that are impossible to corrupt? By definition, they will be impossible to police.

And this is the point at which digital utopians begin to shift uneasily in their seminar chairs.

There's one bleedingly obvious venture where being safe from government matters more than anything else: drug dealing.

The Silk Road catered for all illegal tastes

This is a touchy subject for many people working on legitimate Bitcoin startups, who feel that the Silk Road and other illegal sites have done irreparable reputational harm to the currency, associating it with cocaine, heroin and paedophiles, and therefore putting another hurdle in the way of mainstream adoption.

There has been an ongoing cat-and-mouse game between law enforcement and the founders of these sites. The Silk Road used Bitcoin for payments and hid behind the anonymising Tor network. But it was rumbled when the FBI tracked down the alleged founder and seized his servers. Because there was that single point of failure, it all came crashing down.

But now developers have taken a leaf from the book of Bitcoin and are developing shopping websites which are themselves peer-to-peer.

Amir Taaki is one of a group that recently walked away with the $20,000 first prize in a Toronto Bitcoin hackathon for a proof-of-concept demonstration called DarkMarket. Their idea was to create a fully decentralised shopping service, complete with transaction reviews, a safe escrow service to prevent fraud and user profiles. All of this hangs off Bitcoin's blockchain. There is no server for the FBI to seize, no owner to interrogate and no ISP to demand records from; it's the Hydra of online drug retail.

The developers claim that they won't be finishing it themselves – they're working on other Bitcoin projects. In any case, it would probably be wise not to announce your involvement in launching such a thing. But if it can be done, and demonstrably it can, it soon will be.

A predictable weak link would remain. You still have to post drugs through the mail. This might not bring down the whole marketplace, but it could catch an individual seller if the FBI decide to buy a sample of heroin and use forensics to trace its origins.

This is where the blockchain offers a futuristic solution – for sinister and legitimate retailers alike.

Amazon has tested drone delivery (AFP)

Mike Hearn, a former Google employee who left to work on Bitcoin, described in a recent lecture how the blockchain could be used to form bizarre new autonomous systems that would radically change our daily lives.

He imagined iswarms of drones that could deliver small packages from A to B in an entirely secret and untraceable manner. This would present a huge opportunity for enterprising criminals, but also an enormous threat to the newly privatised Royal Mail and countless other courier companies.

Taxis in the cloud

Hearns described another scenario, set 50 years from now. A fictional character called Jen wants a taxi. She tells her smartphone where she's heading and it immediately starts gathering bids from nearby taxis and ranking them based on price and user reviews. This system on which requests and offers bounce around is called TradeNet, and it would be based on blockchain technology.

The strange thing about these vehicles is not that nobody drives them, as self-driving cars will have become commonplace decades before, but that nobody even owns them. They are what Hearn calls "autonomous agents", independent machines which earn their own money through fares, pays for their own fuel and repair and operates utterly without outside control.

All of this is made possible by Bitcoin. The B-word really is inescapable: it may be only one application of the blockchain but it has proved its power quite amazingly.

Says Hearn: "If I go to a bank and try and open a bank account that is owned by a computer program, they'll tell me to get lost, or they'll think I'm crazy and report me to the police. But Bitcoin has no intermediaries, therefore there's really nothing to stop a computer just connecting to the internet and taking part all by itself.

"All you need to instantiate a Bitcoin wallet is generate a large random number, and pretty much anything can do that. So these devices, they actually earn money and they pay their own costs. And this makes them the first form of artificial life truly worthy of the name."

Google's self-driving car prototype, unveiled in May

These agents could turn to the TradeNet themselves in order to buy servicing, parts or even a whole new car, uploading their own software to it and therefore replicating. They could even hire human programmers to rewrite their code and upgrade them.

Certainly, the very first agent would need to be created by humans. But what car company or taxi firm would choose to do such a thing, given the risk they pose to the bottom line? It would need to be done by the public in order to gain the benefits of ultra-cheap fares, probably following a Kickstarter-style funding model. Handily, that functionality is already built in to Bitcoin.

“There is no such thing as a TradeNet today, but it is theoretically possible,” says Hearn. “Which means that one day someone, somewhere will probably do it.”

Liquid democracy

If you are looking to undermine centralised power, the biggest, most tempting target is government itself.

There are lots of people trying to make inroads into the currency of democratic systems – dollars, sterling, euros, whatever – with the blockchain. Others want to replace state currencies entirely.

Denmark has decided to take a very liberal policy with crypto-currencies, declaring that all trades will be tax-free; profits will be untouched, but losses will be non-deductible. It’s no surprise, then, that this is one of the places it is being experimented with as an election tool.

The Liberal Alliance party, just seven years old, was founded on an ethos of economic liberalism – it supports a flat rate income tax of 40 per cent, for example – and has begun to use technology built on Ethereum for internal votes.

Party spokesman Mikkel Freltoft Krogsholm argued that it was an obvious choice for e-elections because it allows transparency and security and gives people the chance to “look under the hood” of the voting process. “From a liberal ideological point of view, it was an opportunity we just had to take,” he said.

The blockchain makes perfect sense for this application because all transactions (they can be thought of as votes in this scenario) are recorded in perpetuity for reference. It also provides transparency so that a person can check that his or her vote was actually counted. Otherwise, how can you ever really be sure that your paper ballot made it to the final count?

Eduardo Robles Elvira is working on a similar but larger-scale system which he calls Agora Voting. It was developed as a tool for the Internet Party in Spain, which has a policy that all citizens should be able to vote on all matters in constant referenda. Rather than keep the code private he works with any party that wants to apply it to e-elections.

It has already been successfully used in election primaries, with over 33,000 votes being cast.

The ultimate aim is “liquid democracy”: not to just elect representatives and let them get on with it, and not necessarily to have direct referenda on each tiny issue, but to offer a system so flexible that a happy medium can be struck for every citizen.

It can be best thought of as a social network designed not to help you share photographs, play games or communicate with your friends, but to run and manage your country.

If you want to cast your vote on every issue, fine, that’s possible. Or you can place your voting power in the hands of a career politician, as in the current system, or a knowledgeable friend or colleague.

And control could be infinitely fine: say you’re a cyclist, you could hand over voting power on all road safety matters to a cycling charity that pushes for better infrastructure, but retain votes on economic matters and leave everything else in the hands of your local Liberal Democrat office.

“The idea behind liquid democracy is not to remove representative democracy with direct democracy, but to let you choose your means of democracy. You don’t use an airplane to get to the street corner, and you don’t walk from London to Tokyo: depending on what you want to do, you choose the means of transport,” Robles told me.

“We might see in the future a shift from trusting a single entity to trusting a computerised democratic and verifiable system, the same way that we saw a shift from trusting our healers and priests in the Middle Ages to trusting the scientific method.

“It’s just a glimpse into the future. It’s like the first website: it doesn’t have animations, it’s not responsive, it may look now really basic, but still, it’s the base of what we use now everyday, twenty years later. Maybe we will have a system more similar to ancient Athens, but scalable, where elected leaders are not so important.”

It sounds appealing. But how does the blockchain record votes? In basic terms, with Agora, each voter gets some coins (in this case Zerocoins, an add-on to Bitcoin which shrouds transactions in anonymity) and they pay them into an account representing a choice. Imagine a yes/no referendum where the winning option is simply the account with the highest balance.

Again, as with all of these systems, this complex, mechanical stuff will be hidden from plain sight and the user will be presented with a simple-to-use interface, just as we don’t need to know how our mobile phones, the internet or email truly works.

Think of a nation state with an interface like Facebook: do you “like” this policy?

Blockchains versus banks

Andreas Antonopoulos is chief security officer at UK-based Blockchain.info, the world’s largest Bitcoin wallet provider with over 1.1m registered users. Unlike many of the startups here, the company is several years old and already well respected in the Bitcoin community for building useful, reliable tools.

Antonopoulos may be biased, in that case, but believes that the blockchain is one of the most important inventions of the 21st century. He sees it as a force for good, bringing bank accounts and access to international finance to the more than six billion people currently stuck in a cash-only economy. Many Africans have access to mobile phones and the internet, but not banking.

It will also clean up and simplify the banking system.

“Most of the hierarchical institutions we have built around finance are there to regulate the fact that if you give a lot of money and put it under the control of a single person, history tells us that they tend to steal that money,” says Antonopoulos.

“That happens again and again. Almost all regulation is really to stop one person with control over a lot of money from stealing that money.

“This technology makes it largely unnecessary. The end result is that you’re going to see some pretty big changes. Those changes will be because there are now better ways of doing things, and people will choose those better ways. There’s nothing particularly libertarian about that. It’s simply a recognition that you can achieve in software what regulation has failed to achieve.”

Some of this will take the form of banks adopting blockchain technology themselves,

replicating the services they offer now but with more transparency and lower overheads. It will also mean totally open services out of the control of any bank or organisation. Many services are obsolete – they just don't know it yet.

"It's ironic how what terrifies the banks today is actual free market capitalism. They don't like that. They don't like competition. Actually having to compete with smaller competitors that are more nimble and less costly is something that they've been able to prevent for years with the use of regulation as a barrier to entry."

This success in the financial sector will be a springboard to other industries and applications. And Antonopoulos shares the growing consensus that the blockchain will ultimately set its sights on democracy.

"People think Bitcoin is just a better way to do PayPal, and it's not. Just like the internet, it's a platform, and on that platform you can now build an incredible variety of things.

"We can't even imagine what things people are going to build. But just in the last year, from watching the startups in the space, I've been amazed at the range of innovation that occurs when you combine internet, the sharing economy and crypto-currencies.

"This allows forms of self-organisation that don't depend on parties or representative government at all. Representative democracy was a solution to a scaling problem. The fact that you couldn't get a message across Europe in anything less than a couple of weeks.

"Well, that issue of scale has now been solved. So the question is, why do you need representatives? If you ask people who were born with the internet they can't understand why we need them. To a whole generation of people [the phasing out of represnetative democracy] this is already a normal and natural progression. And now we have the tools to do that.

"In my view, and this is probably why I call myself a 'disruptarian', centralised systems have one inevitable trajectory that has been validated throughout history, which is that as the people in the centre accumulate power and control they eventually corrupt the system entirely to serve their own needs, whether that's a currency, a corporation, a nation.

"Decentralised institutions are far more resilient to that: there is no centre, they do not afford opportunities for corruption. I think that's a natural progression of humanity.

"It's an idea that has existed for centuries and has progressively become more and more prevalent. The essential basics of going from monarchies to democracies, from distributing information, knowledge, education and wealth to the middle class, and power to simple people, has been a trend that has lasted now for millennia.

"This is not some kind of libertarian manifesto, or anarchist manifesto, saying that we don't need mechanisms for achieving social cohesion. It's simply recognising that we can create better mechanisms as we solve problems of scale. That's all. It's not some kind of crazy 'we don't need governments' manifesto. It's simply that we can make better governments when we don't concentrate power as much in the hands of a few people.

"As my ancestors in Greece figured out more than three thousand years ago, power corrupts. You can read about that in the writings of the ancient greek philosophers, and nothing really has changed – only that scale of power, and the scale of misery that can be created when that power is wielded to do bad things."

For all his optimism, Antonopoulos is proposing change so radical that it's almost apocalyptic. Other digital utopians go even further.

Daniel Larimer, who is working on a tool called Bitshares to apply blockchain technology to banking, insurance and company shareholding, believes that this new breed of technologies will ultimately render government entirely obsolete.

“I envisage a situation where governments aren’t necessary. That the free market will be able to provide all the goods and services to secure your life, liberty and property without having to rely on coercion. That’s where this all ultimately leads,” he told me.

“The end result is that governments will have less power than free markets. Essentially, the free market will be able to provide justice more effectively and more efficiently than the government can. So, I see governments shrinking.

“If you think about it, what is the reason for government? It’s a way of reaching global consensus over the theory of right and wrong, global consensus over who’s guilty and who’s innocent, over who owns what.

“They’re going to be losing legitimacy as more open, transparent systems are able to provide that function without having to rely on force. That’s my mission in life.”

In his version of the future, identity and reputation will be the new currency. Laws and contracts will be laid down in code and, if broken, reparations will be sought mathematically rather than through law enforcement agencies, courts and prisons.

Those who cannot make good will be victim to “coordinated shunning” by the rest of the network – the whole of society. They will not be able to interact financially or in any other system running on the blockchain. They will be in an “economic prison”. This will extend beyond being unable to make money transfers, because the blockchain will be in control of voting, commerce and communications. Being banished from this system would make life all but impossible.

“There are ways that you can structure society to achieve justice and encourage people to settle their debts,” says Larimer. “There’s a way to give small-town reputation on a global scale. It is ultimate libertarianism.”

Or anarchy, depending on your point of view.

The blockchain is here to stay

What is clear is that the reactionary image of Bitcoin as a volatile, fragile currency for paedophiles and drug dealers is far off the mark. Just as the British pound, US dollar and euro, Bitcoin will be used for all manner of nefarious activities, but will also open up a world of opportunity.

As the first cryptocurrency, it may not last forever. But the blockchain technology which underpins it cannot be uninvented. It has already begun to worm its way into every aspect of our lives, swallowing up authority and distributing it to us via computer programs.

Programmers have already proved that these systems can be created. And logic follows that overheads and costs will be far lower than those of the commercial counterparts – the tottering giants of Facebook, Google, Amazon and so on.

The big problem – and in the world of computers this has been solved so many times before – is that blockchain systems are complicated to use. But soon, they won’t be. And then the masses will swarm towards them, creating a world we barely recognise.

By Matthew Sparkes, Deputy Head of Technology; “The Telegraph”