Geoff Mulgan, November 2014

Data, identity and control: the unfolding revolution in what's private and what's public

In this paper I look at the potential of Bitcoin technologies – which goes far beyond their current use for currency. I summarise some of the issues around Bitcoin in its current form, and where it might be heading.

Any individual or community needs both privateness and publicness. We need to protect what's secret, personal and intimate from the prying eyes of others; and we need ways of ensuring that commitments are carried through, whether these are contracts, marriage vows or debts. It's the combination of these arrangements that helps us protect ourselves against predation, exploitation and abuse. We exist as social entities, embedded in relationships. Purely private worlds and purely public ones would be hell to live in.

The Internet is now shifting in two rather different directions at the same time. One takes us to the Internet of Things – a world of sensors, flows, things talking to each other, and everything being tracked and visible. Privacy is a thing of the past, and if that bothers you, 'get over it', as Mark Zuckerberg put it.

The other direction takes us towards more human control, with encryption technologies allowing us to control our identity and decide what is visible, and to who, or whether to exist through a thick veil of avatars and aliases. Both directions are equally 'determined' by the nature of the technologies underlying the Internet. Which way we go is a matter of choice, not fate.

Given that so much of the internet is funded by the sale of personal data, with all the risks of misuse and theft that brings, it has long been clear that this space – the space where data, trust and identity come together – will be not just a great political and personal battleground, but also a source of business opportunity.

Dave Eggers fictional best-seller *The Circle* centres on a company that has risen to huge success by offering people a way to manage their personal identity. Many others, in the real world, hope that their app could be the one that becomes the default. For contemporary megalomaniacs, the prospect of creating the ultimate, universal common identifier to link up all the other ones is pretty appealing. It's no surprise that this space is attracting idealists and conmen, freedom fighters and hustlers in equal measure.

In a recent piece I set out some thinking on this, and I've had some involvement in projects aiming to solve the problem, including MyDex, one of the Personal Data Stores. Here I suggest how Bitcoin, and new kinds of money, could help us towards a world where we can strike a saner balance between privateness and publicness, the hell of Big Brother in its modern guises, and the mirror hell where the worst abuses are protected by walls of code.

New monies and Bitcoin

Let's start with money and finance. How do we make our finances secure? And how do we take part in lots of financial transactions without opening our lives up to inappropriate scrutiny? The recent study commissioned by Nesta for DCENT provides an overview of the theory and current practical examples of new monies.

A prompt for some of these is the rapid growth of Bitcoin – offering a dream of a decentralised currency beyond the gaze of governments and tax authorities. Bitcoins have fast established themselves as one of the most intellectually interesting, and radical, ways of reshaping how economies work. In the words of Marc Andreessen, Bitcoin 'gives us for the first time, a way for one Internet user to transfer a unique piece of digital property [eg. money, signatures, contracts, stocks and bonds] to another Internet user, such that the transfer is guaranteed to be safe and secure, everyone knows that the transfer has taken place, and nobody can challenge the legitimacy of the transfer'. There is no need for a background of trust, or law, or regulation.

At their heart is a public ledger that keeps a record of any transactions in bitcoin. This blockchain – a computer file recording transactions – is open to anyone to inspect. The system depends on mining – processing that creates new blocks and validates – paid-in bitcoins, a decentralised alternative to the traditional central bank mint. You can buy them at a Bitcoin ATM or exchange, and then keep them either in a physical form (recording the key codes), or in a file, or QR codes on mobiles. Like many other tools, it uses public key cryptography – generating one public key and one private one, the public one describing the account, the private one conferring ownership rights (which are then lost if the key is lost).

Bitcoin has quickly accumulated friends and enemies. The enemies include Paul Krugman who called it evil, and Robert Shiller, who sees it as a bubble. Perceptions are coloured by the overt political agenda of some of Bitcoin's backers who advocate it as a libertarian alternative to states, and such ugly things as taxes and welfare systems. In the real world it's suffered from volatile prices, the bankruptcy of one of its main centres, the arrest of key individuals, and plenty of fraud.

Yet despite the setbacks, Bitcoin enthusiasts expect it to grow as a currency, helped perhaps by future financial crises, with a value (in the not too distant future) equivalent to tens of billions of dollars, sitting alongside existing currencies. This growth, they argue, could be helped by some compromises with the authorities: offering identity links ('know your customer'), consumer protection and the like.

As a money, Bitcoin raises some important questions, not just about its viability. The most important is: what monies do we need?

Here is a rough list of types of money that have been underprovided by the existing, rather costly, financial system:

- Monies that can be cheaply remitted across borders (currently remittance is a far more important flow than aid, yet remitters pay 10 per cent+ for the simple act of sending money home, an absurd sum in an era of digital technologies)
- Monies that can be cheaply transferred within countries without well-developed financial systems (even the best recent tools like MPesa remain pretty costly to use, again often with 10 per cent+ fees)
- Monies for the unbanked, who still number many millions even in developed societies, who pay a lot for credit of any kind, and who need money that combines the ease of use of cash with some greater security and flexibility
- Local separate currencies that allow the circulation of value within communities (in the tradition of Wörgl, LETs and timebanks) where the mainstream market has failed to keep resources adequately utilised
- Specialist monies that link supply and demand of particular commodities from fiat money, such as care for the elderly (like Japan's Furai Kiippu), again, where mainstream markets or welfare systems are failing
- Welfare monies that specify what the money can be spent on: e.g. requiring spending on food, or local produce rather than beer and cigarettes, or for that matter heroin (a use for which Bitcoin is, paradoxically, particularly well suited).
- B2B monies in localities or on larger scales, as in the WIR, Sardex or Nanto
- Money that is managed in ways that enable people to borrow cheaply against future income, as set out in Nick Gruen's recent Nesta paper 'Central Banking for All'.

I'm sure there are many other examples. I'm also sure that 90 per cent of mainstream economists will be very sceptical of the idea that other monies should compete with traditional fiat currency. Yet the current banking system, which is given unique privileges to create and manage money, now costs some $600bn each year in subsidies, according to the IMF.

The economics profession may be right that no possible alternative could be superior. They may be right that all of the current problems can be solved with changes to banking regulation, and the creation of vast amounts of new money through quantitative easing, rather than reforming money itself. But their claims are based on speculation not evidence. That's why we need some experimentation in relatively safe spaces. Each of the possible monies listed above could be the subject of experiment, comparing alternative models and testing out their efficacy.

And almost certainly some of the experiments may find that Bitcoin, or Bitcoin-like monies, have uses after all, and not just for organised crime syndicates, and could greatly lower the costs of handling money.

Bitcoin beyond money

But if Bitcoin opens up important debates about money it also has much broader implications. A growing consensus sees Bitcoin more as a technology than a currency – a truly radical way of organising economic activity, with guarantees of both control over identity and the publicness of transactions: more private and more public at the same time.

What's most intriguing is that there are now so many permutations. From the libertarian view, Bitcoin looks like an alternative to state control. But it can be used in an almost opposite way – providing a detailed account of individual transactions for surveillance. The public ledger can be organised with no links to personal identity or with prescribed links – there is infinite variety in the potential uses of Bitcoin.

The most obvious use is for the ledger to manage legal contracts or commitments of various kinds, existing in a public space but with privacy protections. This could be a very valuable breakthrough, particularly in countries with very expensive legal systems and opaque contracts. Bitcoin could be used to support voting – particularly in countries where there are concerns about fraud – allowing validation by independent observers.

It could be used for health records or educational CVs – in each case combining privacy, a secure home for data, and scope for external or third party validation. It could be used for handling personal relationships, as an alternative to Facebook. Creative innovation around Bitcoin has only just started.

Close cousins of Bitcoin offer ways of managing personal identity, with authentication separated from authorisation. This is where the personal data stores come in, and projects like 'Open Mustard Seed'.

These offer the prospect of 'zero knowledge proofs'. For example, if I'm renting an AirBnB apartment there is no need for the lender to know who I am; they only need to know that I will pay, and that if there is a problem they can then find a real person, for example for redress if I wreck the place. The same is true of most commercial interactions. There is no need for Tesco or Walmart to know who I am either, and I would much rather they, and a clutch of other big businesses, didn't know the contents of my shopping trolley.

More savvy citizens and consumers will surely want to see new arrangements (ones which protect identity, rather than sharing it around carelessly) become the default, and if businesses don't take the lead they will surely ask governments to legislate.

And so out of Bitcoin, and an associated range of innovations around the intersection of data, identity and trust, we may begin to see a different landscape taking shape through the mist, a landscape that is neither one of complete anonymity, or one in which big organisations have an automatic right to know who we are.

This is a classic example of a field where technologies will co-evolve with regulations and policies. Once again we will learn that simplistic accounts, in which technology causes change in a linear, deterministic way, turn out to be wrong.

Handled right, a thoughtful co-evolution of technologies and rules should be progress. Handled right, it may make us freer by making our world both more public and more private at the same time.