The Future of Digital Currency. Will Bitcoin change the world?

by Gareth Williams

Bit Trade Australia Essay Competition

First place award

BitTRADE AUSTRALIA
THE EASIEST WAY TO BITCOIN

Digital Currencies and the Future: Will Bitcoin change the world?

There is a new force in the world today. Many people may not yet recognise it, but the marriage of two very powerful ideas, trustless cryptographic transactions and distributed consensus systems, is a technological storm set to sweep the globe. Much like its predecessors - the personal computer, and later the Internet, the foundations upon which it builds - Bitcoin's significance can not be overstated, nor fully anticipated in advance.

Forget what you've heard about Bitcoin's supposed objectives, or those attributed to its anonymous creator. It's as absurd to suggest that Bitcoin aims to help people evade taxes or buy drugs anonymously as it is to suggest that the Internet "aims" to do those things. The network is neutral; politically agnostic. It's just infrastructure, and it's entirely open and public. You need trust no one, nor agree with anyone's politics, in order to participate as an equal peer. Now that the genie is out of the bottle people will inevitably use this technology for anything and everything that it is capable of.

So, what is it capable of? Very broadly: replacing troublesome, expensive, corruption- and failure- prone humans with trustless cryptographic protocols.
"Trustless" is a somewhat counter-intuitive term. Your average man on the street hears this and immediately thinks of the opposite of institutions like his bank or credit card company, in whom he trusts implicitly. "And what's wrong with trusting them?" he may justifiably ask. "Why should I want to do business without their involvement - isn't that risky?"
The answer lies in our definition of "trustless". Trustless doesn't mean we remove the trust itself - rather, it means that we remove the need for trust. Consider it a synonym for "failure-proof." This is a very powerful concept. When your system bypasses an entire class of problems so reliably that they simply cannot occur, then the need to employ someone to manage those problems for you disappears. This removes not only the cost of the middleman, but also common failure modes associated with humans - honest mistakes, corruption, etc.

Consider gambling for a moment. A problem gambler can spend hours feeding money into a pokie machine before the house edge inevitably wears him down. It doesn't help that the pokie machine operates as a black box, often having an unexpectedly high and completely unknowable house edge. Some have even been rumoured to engineer results tailored to individual players in order to influence their behaviour. Endless arguments could be had as to whether our man is being exploited, or simply exercising his right to spend his money as he sees fit. The government certainly spends a bit of money as they see fit, on education campaigns and services attempting to address this social problem. But can we actually change the addict's behaviour? One thing is undeniable - the people who profit from this state of affairs have a vested interest in maintaining the status quo.
What if we could do away with the poorly-incentivised (from a general welfare point of view) middlemen completely, instead allowing the gambler to play a fair game - 50/50 odds, no house edge - against another willing gambler. There could be no allegation that one of them is exploiting the other. The gambler could still spend his money as he saw fit, and would obviously be attracted to a game with zero house edge. Suppose that he played this game for a long time - placing frequent bets for hours at a stretch, as problem gamblers are observed to do with pokie machines? The statisticians in the audience will note, with a wry smile, that our gambler is likely to end up back where he started. Flip a coin a thousand times and you'll frequently get close to 500 heads, 500 tails. The software that enables this game, peer-to-peer over the Internet of course, could even have an "auto bet" feature baked in - just switch it on and come back later to see if your balance has changed

much after a few thousand bets (it won't have.) That may not prove so addicitive. If such a

system were to become widespread, and to push pokies out of the market, it could accomplish something that governments have largely failed to achieve.
How could we go about building such a system? Well, up until 2009 the answer was “we can’t.” You’d always have needed a middleman to handle the money, whose incentives don’t naturally align with the those of the gambler or of society at large, introducing the same old problems outlined above. Now, there do exist cryptographic protocols that allow two people to perform a fair coin flip (or dice roll) at a distance, trustlessly, with no possibility of cheating. All we need is a way for the money to change hands: enter Bitcoin. Now we can design a trustless protocol that allows two strangers to flip a coin over the Internet without a middleman, without having to trust each other, and with a mathematical guarantee that the winner will always receive the amount wagered from the loser. The other pieces of the puzzle are a common communication channel and a pairing mechanism that matches bets against one another, both solved problems. The only reason that this system does not exist today is that nobody has coded it yet.

Just let that digest for a moment. It bears repeating. There exist hundreds - probably thousands - of simple but potentially revolutionary ideas, just like this one, that very suddenly don’t exist only because someone hasn’t coded them yet. Five years ago they didn’t exist because they were either impossible, or involved prohibitively expensive or complex interaction with middlemen. Bitcoin enables - as Vint Cerf famously said of the Internet - permissionless innovation. You don’t need to sign a contract with anyone to build stuff with Bitcoin; you just need to write the code. A whole class of really hard problems have suddenly been reduced to just programming problems. And, oh boy, we know how to solve those.
Imagine a peer-to-peer stock exchange. No brokerage fees. No broker. No barriers to entry - anyone in the world can float a company and issue stocks, which participants in the market are free to purchase if they have confidence in the issuer. Trades are atomic and guaranteed. Ownership of stocks is cryptographically secure. It doesn’t exist only because someone hasn’t coded it yet. A reliable, open, free document time stamping service. A decentralised name registration service. Micro-payments - something that could drive whole new monetisation models on the web, or finally enable large scale mesh networks (by incentivising people to run nodes with automatically adjusting micro-payments for traffic in/out.) All awaiting implementation, or at least a friendly UI. The list is endless.
Bitcoin does a lot of exciting things really well right now too. The ability to shift arbitrarily large amounts of value to arbitrary points on the globe in minutes, for virtually free, is nothing to sneeze at. Foreign workers from impoverished nations remitting money back home stand to benefit from this enormously. They now have the power to make an end-run around the exorbitant Western Union tax, ensuring a greater portion of their income makes it back home. The extra wealth flowing into some of these small nations will directly help to lift people out of poverty.

Another thing that will lift people out of poverty is unrestricted access to the global marketplace. Trade can make or break a nation. If your nation happens to be one of the ones the traditional payment networks don’t do business with - either due to excessive fraud (Nigeria), government sanctions (Iran), or just generally having an economy too small to care about - then you’ll be forced to flog those coffee beans you grow off to a middleman, for cents on the dollar, because he has access to marketplaces and capital investment that you do not. Some people would call that exploitation. Others would just call it an uneven playing field. In any case, Bitcoin goes a long way toward leveling that playing field. Our impoverished coffee grower can put up a website and sell his coffee beans directly to global consumers. If he needs capital, for example to purchase a roasting machine to help him add value to his product, he can solicit micro loans. Or even issue shares in his business on that global peer-to-peer stock exchange we discussed earlier, once it exists (and it will; programming problem.) He may need to find people who can vouch for his authenticity before anyone will have the

confidence to invest in him, but that's a low bar compared to his current situation. Bitcoin is banking for the world, accessible to anyone with a smartphone.
With all these applications the world is already looking pretty different, but it doesn't stop there. Like the Internet, Bitcoin's censorship resistant properties are a boon for democracy - financial freedom to accompany the freedom of information we've become so accustomed to. Wikileaks, for example, recently revealed that the majority of donations they receive are in the form of cryptocurrency.

Smart people are already working on even more way-out-there concepts than anything discussed thus far, such as the "Decentralised Autonomous Corporation." Having made the observation that a public company's behavior is largely governed by people (directors) following a set of rules (algorithms) to achieve a set of clearly defined outcomes (maximise profit,) it was inevitable that someone would ask the question: "can we do away with the people, and just stick with the algorithms?" From the industrial revolution onward machines have gradually replaced human labour at the bottom end of the pay scale, improving living standards for everyone. Thanks to Bitcoin people are finally able to dream of automating human labour at the top end of the pay scale. When a computer program first employs a human - as always to perform the most creative work, which the machine is incapable of - then we'll really be living in a different world.

Could Bitcoin be superceded by something else one day? It's certainly not impossible, although this would do nothing to mitigate the world-changing effects this technology is destined to have. It would appear, however, that the odds are heavily stacked in Bitcoin's favour at present. Bitcoin is, at heart, a distributed consensus system. Both upper-case-B Bitcoin, the technology platform, and lower-case-b bitcoin, the currency which is traded atop it, have been cleverly designed to nudge all participants toward consensus through economic incentives. Bitcoin mining is something with a strong "network effect" - an individual stands to gain the most by working on the same blockchain as everybody else. Currencies also experience this network effect - an individual gets the most benefit from using what everybody else is using. Bitcoin enhances this effect with a fixed money supply; individuals are incentivised to acquire and hold a currency whose value is appreciating, and this behaviour in turn drives further appreciation. As a bootstrapping mechanism, to get us from zero to worldwide use, you have to admire the elegance of this.
Bitcoin is, and has the momentum to remain, the premier global cryptocurrency. The further ahead it gets the more users it will attract, while altcoins and perhaps even national currencies are gradually deserted like orphaned blocks belonging to a chain that diverges from the consensus (quite tellingly, this is all many altcoins really are - a fork of Bitcoin's blockchain from block zero, destined for abandonment as the entire ecosystem drifts back toward consensus.)
The power of a global currency to facilitate trade is hard to understate. Just as the Internet famously "interprets censorship as damage and routes around it", Bitcoin interprets a world full of splintered national currencies as a consensus problem and incentivises convergence. With the inevitability of an idea whose time has come, Bitcoin's star is rising. A decade from now the world will be unrecognisable.

You can't stop the signal.

Gareth Williams