

5 December 2014

Dr Kathleen Dermody, Committee Secretary  
Senate Economics Committee PO Box 6100  
Parliament House  
Canberra ACT 2600

Dear Dr Dermody,

Re: Senate Economics Reference Committee Inquiry into digital currency.

I write in response to your letter dated 14 October 2014 inviting a submission to the Inquiry into Digital Currency. I appreciate the opportunity to provide comments on digital currency.

Currently I'm a full-time software engineer working at Atlassian<sup>1</sup>, Australia's most successful and fastest growing software company<sup>2</sup>. I've worked there for about nine years and have seen the company expand globally, opening new three offices this year alone. What was only twenty-something people in a single room in 2005 now expects to hire over 600 staff in the next 12 months, most of them in engineering roles like myself. If only we could find enough Australian talent to fill all of those roles at our main office in Martin Place, Sydney.

Researching Bitcoin since late 2011, I have developed software, written many articles, spoken at Bitcoin conferences in Australia and New Zealand and consulted to Bitcoin businesses. I am deeply engaged with the Bitcoin community globally and I coordinate a Bitcoin meet-up group in Sydney. It has taken me a considerable amount of time to arrive at my current understanding of Bitcoin and its potential. Like most, my initial thoughts were that it must be a scam or at best another hopeless dream like the previous two decades of unsuccessful digital currency projects I witnessed.

Back in 1981 at eight years old, as I began computer programming, I realised the personal computer would change the world dramatically. I tried to convince everyone around me that the computer revolution was coming but nobody seemed to believe that the fledgling hobbyist devices of that time would ever exceed their obvious awkward limitations to become essential for everybody, everyday nor that they could be a creative tool for artists and musicians. Computers were then only considered the domain of big business or big science.

---

<sup>1</sup> "Atlassian named Australia's best place to work" BRW, 11 September 2014  
[http://www.brw.com.au/p/leadership/atlassian\\_named\\_australia\\_best\\_place\\_p3XQE2CmYvpJbn2XejGnHJ](http://www.brw.com.au/p/leadership/atlassian_named_australia_best_place_p3XQE2CmYvpJbn2XejGnHJ)

<sup>2</sup> "Atlassian's Sales Rise 44% to \$215 Million" Wall Street Journal, 10 September 2014  
<http://blogs.wsj.com/digits/2014/09/10/atlassians-sales-rise-44-to-215-million/>

When commercial internet hit Australia in 1991 I recognised a new stage in the computer revolution. This was no chaotic, unpredictable populace on the rampage. This revolution was like the scientific revolution; a quiet yet transformative increase in human capability. The media at the time focused on “Internet the Drama” - after all, the instructions to build bombs were available to anyone and the publication of illicit material was no longer effectively blocked by ratings imposed or refused by The Classification Board. In the two decades since then we have seen over two billion people join this global communications and information system and doing so costs far less than a textbook.

Bitcoin is a third stage in this computer revolution. It’s still in its infancy but is growing fast and many of us are working to accelerate this. In 2014 the speed of innovation in **Financial Technology (FinTech)** is very high, much higher than that of smart phones or the internet itself when it was new. The fact that Bitcoin is *fully decentralised* crucially enables accelerated growth whereas centralised coordination adds friction and cost to innovation.

## Is Bitcoin a Threat or Opportunity?

The digital revolution has disrupted many industries, but none quite so big and powerful as financial services. We should all expect incumbents to attempt to protect their privileged market dominance. Banks, credit card companies, money transmitter businesses to name a few, all these companies will come to realise they ultimately need to drastically change their businesses or they will suffer on the bottom line. Jamie Dimon, CEO of JP Morgan recently identified Bitcoin as a significant competitor<sup>3</sup>. Payments systems trade journals discuss the oncoming “margin squeeze” due to both tech giants like Google and Apple and by platforms like Bitcoin.

You will hear that Bitcoin is a fantastic *opportunity* as I detail below, however Bitcoin is also clearly identified as a *threat*. What is not always clear, however, is who it is a threat to and how that threat arises from some open source<sup>4</sup> computer code.

Bitcoin is not suitable for crime in comparison to cash. Bitcoin is not as good for terrorism, money laundering or tax evasion as cash. Bitcoin is fully traceable - “an auditor’s dream”. In fact the extreme transparency of Bitcoin has many privacy activists quite worried. The fact that the global ledger of all Bitcoin transactions is publicly accessible means investigative police work is better supported by Bitcoin than by cash.

The transparency of this ledger offers many benefits from transparent accounting in charities to reduced opportunity for undetected corruption and embezzlement both in government and private corporations.

---

<sup>3</sup> “Big Banks Are Confident in the Face of the Bitcoin Threat”, Institutional Investor, 10 October 2014  
<http://www.institutionalinvestor.com/inside-edge/3389462/big-banks-are-confident-in-the-face-of-the-bitcoin-threat.html>

<sup>4</sup> Wikipedia [https://en.wikipedia.org/wiki/Open\\_source](https://en.wikipedia.org/wiki/Open_source)

The main threat Bitcoin represents is *disintermediation* - cutting out the middlemen - just as going digital has done in so many sectors: media, publishing, communications, music, film. Just ask Kodak.<sup>5</sup>

Incumbents will resist change. They will fight against Bitcoin. They will fight for what is best not for Australia, but for themselves.

Bitcoin is competition for legacy financial services companies because it automates many of the manual processes through which they provide value. This technology does it far cheaper by eliminating third party risk. Bitcoin cuts these third parties out of many kinds of transaction and it minimises their role in others.

The biggest unknown with Bitcoin is the positive potential. Who - given a time machine - could resist the opportunity to travel back only a decade or so to a world still skeptical of “the internet fad” and buy some stock in a startup called Google, now one of the worlds largest companies?

Just as we couldn't imagine Google before the web, we can't imagine the value that will come from the underlying technology of Bitcoin. This **blockchain** technology is not merely a new version of what came before. It is a totally new capability and nobody knows exactly where it is capable of taking us.

Over the past few years I have gradually become less skeptical and more bullish about Bitcoin. I now recognise Bitcoin represents a new software technology category. Money is just the first example of its capability, like email was the first “killer app” of the internet. The best is yet to come.

## What's in it for Australia?

Australia has a unique opportunity to take advantage of digital currencies and blockchain technology. Our remoteness from trading partners is a diminished limitation in this internet age. We have solid education and access to the fastest growing markets in Asia. We are willing early adopters of technology, have a sophisticated financial services workforce and a stable economic and political base, not to mention the weather and lifestyle!

If Australia fumbles digital currency technology, we will have no excuses, no-one to blame but ourselves.

Australian FinTech startups begin with this natural advantage and digital economy companies worldwide already identify Australia as a potential base of operations. They also see a healthy economy and a rich, accessible market opportunity<sup>6</sup>. Lack of regulatory certainty is a commonly-cited risk factor and many jurisdictions seek to attract that

---

<sup>5</sup> [https://en.wikipedia.org/wiki/Eastman\\_Kodak](https://en.wikipedia.org/wiki/Eastman_Kodak)

<sup>6</sup> “Australia: The Hottest Bitcoin Market on Earth”, Cryptocoins News  
<https://www.cryptocoinsnews.com/australia-hottest-bitcoin-market-earth/>

business while the sector is still small. London, Singapore, Isle of Man, Jersey, Panama and many others have clearly recognised the opportunity and this is reflected in their appropriate regulatory response to Bitcoin. Australia can do this.

If Australia provides an appropriate regulatory environment that encourages early stage innovation, Aussies who have had to leave to build their businesses will be encouraged back to Australia where they'd rather be, as will highly skilled foreign operators, both of whom are essential to building practical skills in our workforce that high technology relies upon. The controversial backlash against tertiary education within startup culture is predicated on a truth that technological leadership is primarily coming from agile innovators and not the hallowed halls of prestigious educational institutions.

## Consumer Protection Built-in to Bitcoin

Financial services are regulated around the world with a few important goals. We cannot expect to take existing regulation of financial services, and merely copy and paste for Bitcoin. The ideal path forward is to keep these goals in mind when learning about the differences and similarities of Bitcoin and traditional financial services.

One regulatory goal, **consumer protection**, is crucial whenever a business takes custodial control of a consumer's money. Bitcoin enables this, and the infamous failure of Mt Gox<sup>7</sup> shows only that when a company has custodial control of its customers' money (both fiat currency and bitcoin), the custodian's incompetence, negligence or criminal intent can result in massive losses of customer funds. In fact, without functional consumer protection, this outcome is seemingly inevitable, just as we see in the case of even more expensive high profile bank failures<sup>8</sup>.

The regulations for consumer protection **ought not be a blanket rule smothering businesses that do not have custodial control of customer funds.**

Bitcoin offers new options not commonly found in legacy banking. What follows is an example of one Bitcoin feature, how it offers a superior service and how this service should be considered when designing regulation.

## How Multi-Signature Makes Bitcoin Better than a Credit Card

Bitcoin transactions are authorised through digital signatures. Rather than signing with a pen, under the hood, digital signatures are made with secret codes called keys<sup>9</sup>. Bitcoin

---

<sup>7</sup> "Mt Gox: The brief reign of bitcoin's top exchange", Reuters, 28 Feb 2014

<http://www.reuters.com/article/2014/02/28/us-bitcoin-mtgox-insight-idUSBREA1R06C20140228>

<sup>8</sup> [https://en.wikipedia.org/wiki/Bear\\_Stearns](https://en.wikipedia.org/wiki/Bear_Stearns)

<sup>9</sup> A cryptographic key is created randomly and is numerically unique. This is the basis of all modern cryptography and digital signatures used for authentication in everything from bus tickets to nuclear missile launch silos.

keys can be stored on your mobile phone or laptop, in dedicated secure devices, even printed on paper. The terminology is confusing, but a private key functions just like car keys. You need the car key to drive your car. In the case of Bitcoin, this is a mathematically enforced rule with no chance of “hot-wiring” like in the movies. You must possess the private key in order to sign a transaction. Bitcoin’s multiple signature scenario, like a joint bank account, requires more than one signature to execute transactions.

Multi-signature features added to Bitcoin in the past few years enable a financial services company to provide risk assessment services for electronic payments in much the same way as credit card companies actively monitor their customers’ transactions today. Those transactions that fail to match the customer’s legitimate pattern trigger an alarm. However, credit card companies also execute the transaction on their payment network and have full access to customer funds and identity, so in this case the credit card provider is playing multiple roles: payment network, risk assessor, identity manager, and credit facility. The credit card company competes against other companies who offer the same bundled product. It’s a job lot.

Credit card companies can offer their demonstrated expertise in risk assessment to Bitcoin users in a signatory role for transactions initiated by the customer. In this scenario the customer would always maintain control of the funds through their control of two out of a possible three keys while the risk assessor would hold one. In this example of multi-signature transactions, two out of three signatures are necessary and sufficient to complete a transaction.

In this scenario the customer would hold one key in their “wallet”<sup>10</sup> and the other, say, in a safe or bank deposit box. The customer alone has full control of their funds. They play this role and assume responsibility for theft or loss. The customer would sign transactions with their main key only and the risk assessment service would respond by signing with their key - unless there seemed to be a problem. Just as credit card companies call customers to check suspicious transactions, so could they do this with Bitcoin.

It’s worth noting that many variations on this theme are possible and the development of these would be encouraged in an environment of open competition among innovators as opposed to one full of onerous regulatory barriers to entry and a few slow-moving, monolithic oligarchs. The risk assessment service could also allow the customer to set daily spending limits. The number of keys required to complete a transaction does not have to just be two-of-three; it could be seven-of-ten or fifteen-of-twenty etc. with multiple parties involved such as in the joint bank account of a couple, parents monitoring kids’ pocket money or corporate treasury management.

The primary difference between this kind of multi-signature transaction and credit card companies’ current operation is that no kind of operational failure (security breaches, malfeasance etc.) within the credit card company can ever result in loss or theft of the customer’s Bitcoin funds. The company has no custodial control of those funds. As long as

---

<sup>10</sup> The typical name of a Bitcoin app on your smart phone or computer is a Bitcoin Wallet. This is where the user’s private keys are stored securely.

Bitcoin works at all, it's just not possible. Consequently, that impossibility no longer needs to be insured against, remediated, mitigated or regulated. This is the precise origin of the cost and efficiency benefits. The extent of the risk assessor's power is to either sign a transaction or to not sign it. Such a service would be offered for a small fee to the customer who gains protection from the theft and abuse of their main key.

The third key, kept in the customer's safe, is reserved for when the customer wishes to recover from either loss of the first key (although keys should be backed up) or more importantly, in the event of any failure of the service provider's operations or business. In this example, consumer protection is clearly superior even while being cheaper.

So on the matter of consumer protection, while it is crucial to regulate those businesses who maintain custodial control of customer funds in exactly the same way as traditional financial services companies currently are, that regulation cannot equally apply where there is no custodial control. Clearly a risk-assessing signatory should not be subjected to expensive compliance with regulations to prevent them from doing that which is made mathematically impossible by Bitcoin.

There are many important consequences for maintaining this distinction in any financial services regulation that covers service providers involved in Bitcoin multi-signature transactions:

1. Neither customers nor merchants have to share the cost burden of credit services that have a history of high rates of transactional fraud and frequent cases of hacking and other security breaches resulting in the loss of their credentials.
2. Customers can choose an appropriate level of risk protection for the transaction. Small value transactions such as a sandwich are not worth the overhead. Today the frequent experience is a minimum transaction amount or a \$1-\$1.50 fee which represents more than 10% of the transaction value and prevents customers from using cards for smaller transactions. Conversely very high transaction amounts can be appropriately loaded with additional due protection.
3. Existing companies with risk assessment expertise - like credit card companies - can offer this service to customers they would not extend credit to. The unbundling of the risk assessment from the credit is a new revenue stream for these companies.
4. People with poor credit scores who may stand to gain from fraud protection but for whom the extension of credit is too high-risk can benefit and still escape the financial hardship from poor credit management.
5. Companies with risk assessment expertise who do not have the capability to offer credit can directly access and compete in this market.
6. Risk assessment expertise can be targeted for relevant specialities such as rare coins and stamps, antiques and other specialist goods and services. **Both consumer and business customers can benefit from a higher value service that incorporates deeper knowledge of the product domain.**

7. Regulatory oversight is an expensive compliance cost that adds no value to risk assessment, only to the extension of credit. The reduction in this cost is an efficiency gain shared throughout the economy.
8. Consumer privacy can be greatly improved by reduction in the necessity to credit check and background check for individuals who might otherwise pose a credit risk. As they are not being offered credit services, the burden of vetting them for this purpose is not required.
9. Consumers' identity details do not need to be collected and shared among so many parties so the burden of attempting to secure large caches of personal data is reduced and in some cases eliminated entirely.

Bitcoin is programmable money. While multi-signature transactions have received a detailed treatment in this submission, this is only one of the many capabilities Bitcoin enables. Also, the multi-signature features of Bitcoin provide many other examples which demonstrate dramatic improvements in efficiency and security. Some of the consequences of those include:

- Further reductions in identity theft for consumer transactions;
- Reduced costs in supply-side risk with untrusted product suppliers;
- Reduced fraud rates for suppliers;
- Integration with automated delivery tracking as a secure and efficient "cash on delivery" model that does not entrust the courier with the funds.

The list goes on.

In order to appreciate the full range of possibility, research and development must continue, and importantly, small businesses must be allowed to innovate so that products can be tested in the market.

## An Appropriate Regulatory Response

Knee-jerk reactions to regulation fuelled by headlines and hysteria will obviously endanger innovation in Australia and push FinTech companies off-shore. We have seen this happen <sup>11</sup> since the ATO preliminary ruling on the applicability of GST to Bitcoin as a taxable supply failed to recognise Bitcoin as money under the GST Act.

Globalisation is no more prominent than in internet-based businesses. Their operations can very easily relocate, as can their profits.

Ultimately, if Bitcoin is what we think it is, we will need legislation that is not confined by the misguided question of whether Bitcoin is a commodity or a currency. This is like asking if the internet is a telephone or a postal service. Bitcoin has properties of currency and

---

<sup>11</sup> "Aussie Bitcoin start-up CoinJar moves to the UK", The Australian, 2 December 2014  
<http://www.theaustralian.com.au/business/latest/aussie-bitcoin-start-up-coinjar-moves-to-the-uk/story-e6f rg90f-1227141173086>

commodity simultaneously and yet it's a square peg that fits in neither of those two round holes.

Further, Bitcoin the currency is only one of many examples of this particular kind of “digital bearer instrument”. The full menagerie of equity classes from the exotic to the mundane can now be created in pure software thanks to the groundbreaking innovation of blockchains and distributed consensus networks<sup>12</sup>. Thousands of companies and probably tens of thousands of software projects are already seeking to build these.

Counterparty<sup>13</sup> is one such project that builds on top of Bitcoin's blockchain and enables anybody (not just programmers) to create “equity tokens” with a few clicks of the mouse and a small fee in bitcoin. The economic parameters (issuance schedule, total monetary supply, inflation curve etc) as well as the ultimate meaning and value of the token are established by its creator. All such tokens can be traded freely without the involvement of the original creator. Typical examples are crowd-funding tokens issued by musicians<sup>14</sup>, loyalty points or novel crypto-currencies such as GenerCoin<sup>15</sup> where each token is asset-backed by 10,000 BTUs of renewable energy, redeemable at any time from its issuers.

The important lesson here is not whether all these financial novelties will hold a value. It's probable that many of these projects will fail. What's important to recognise is that we are at the beginning of a FinTech Renaissance and we should choose wisely how we respond to a rare opportunity.

As software technology is a high growth area with an open-ended future, Australia has an opportunity to go beyond the heavy primary industry of the past, being subject to fluctuating commodity prices, selling dirt. Australia's failure to nurture the tech sector has already seen many high growth Australian startups seek venture capital in the USA where valuations reflect a more sophisticated and informed investor community. The fact that these investors are typically co-located at the epicenter of software technology, Silicon Valley, is clearly a reflection of the cooperation and communication between R&D, business and finance. Why do so many Aussie innovators have to go to Silicon Valley to realise their potential? Why do they list on the NASDAQ instead of the ASX? What needs to change?

---

<sup>12</sup> Bitcoin's network is distributed - it arrives at consensus about the state of the ledger (blockchain) without central control. This design is well suited to a broad range of applications for which we have become accustomed to heavily rely on a vetted central arbiter or entrusted authority.

<sup>13</sup> <http://counterparty.io/>

<sup>14</sup> <http://tatianamoroz.com/tatiana-coin/>

<sup>15</sup> <http://www.genercoin.org/>



## Bitcoin Security

*Upon his capture in 1934, the legendary bank robber Willie Sutton was asked by FBI agents, “Why do you rob banks, Willie?” Sutton, who believed the question to be rhetorical, replied, dryly, “Because that’s where the money is.”<sup>16</sup>*

Information security is universally poor in 2014. No organisations demonstrate an ability to secure valuable data, such as their own customers identities and credit card numbers or their state secrets. Those that have not been hacked are expected by most information security professionals to be hacked before long. While it is built using time-tested cryptographic technology, the same stuff that secures military and banking systems around the world, the Bitcoin *network* is a more secure system.

How can this be?

Individual Bitcoin holders such as myself are not harder to hack than a large merchant’s database. We are likely much easier to target for theft. The major difference is that a large merchant database of sixty million credit card numbers, such as US retailer, Target, lost in a recent high profile breach, Target was a target sixty million times sweeter to any attacker than a single individual, yet the security systems at Target are not sixty million times stronger. Even if they are six times stronger, that’s still a million more reasons for an attacker to target them rather than me.

This situation is commonly referred to as the *Piñata Effect* because all the goodies are collected into one tempting target, like the cardboard donkey full of lollies at kids parties.

This model of information security is *broken by design*. It cannot be improved by merely adding more layers of colourful paper to the donkey. Bitcoin’s distributed network has a fundamentally different design.

Bitcoin’s security model is new; we have never had a system that is both secure and decentralised. These two attributes were always assumed to be at odds until a famous long-standing problem in computer science, **The Byzantine Generals Problem**, was solved in Bitcoin by *Satoshi Nakamoto*, the pseudonymous creator of Bitcoin<sup>17</sup>. This problem defined the task of ensuring accurate communication through and among *untrusted* parties about the true state of - in this case - a transaction ledger. Centralised cryptocurrencies have been around for decades and never reached maturity since the central party was too easy to shut down or too hard to trust. Bitcoin does away with a trusted central coordinator entirely.

---

<sup>16</sup> Selected Works of William Bradford, [http://works.bepress.com/william\\_bradford/1/](http://works.bepress.com/william_bradford/1/)

<sup>17</sup> “Bitcoin: A Peer-to-Peer Electronic Cash System”, Satoshi Nakamoto, <https://bitcoin.org/bitcoin.pdf>

## How do We Know Bitcoin is Secure?

Surprisingly, the fact that Bitcoin's creator is not identified is not considered any kind of danger to Bitcoin's security because Satoshi is not a trusted party in Bitcoin. Nobody is. The software that he or she created is open source, meaning there are no trade secrets and the nuts and bolts are open to public scrutiny<sup>18</sup>. Since it was handed over to others in 2010, most of the code has been rewritten through the continual process of upgrading and improving it in public through open collaboration.

Satoshi has no control of Bitcoin, any more than any other network participant<sup>19</sup>. Financial services' security models have traditionally relied upon limiting access and carefully vetting any parties before they may connect. Bitcoin is the opposite. It has been designed with the full expectation that there is zero trust between the participants and that they will tend to act in their own self interest. This turns out to be a reliable assumption and removing the need to trust participants enables opening the network to everyone.

Bitcoin's security is based on the opposite approach to traditional dysfunctional information security. Rather than protecting the system from attack by limiting the access of attackers, Bitcoin has been consciously battle-hardened, exposed to continuous attack since its creation. This ensures that the only system able to arise successfully is one maximally tested against the widest possible range of available threats. This makes Bitcoin **antifragile**<sup>20</sup> - the more it is attacked, the stronger it evolves to be.

So how do we know Bitcoin is secure? Because there are several billion dollars of value at stake which the network has protected for years without controlling access or limiting knowledge about its inner workings. While individuals' computers and various entrusted companies' systems have been hacked (as in the world of credit cards), Hackers are continuously trying to crack the Bitcoin *network* security and they have not made any progress.

## Is Bitcoin Money?

Yes. Bitcoin is money. It was designed to be money and is well suited as money. The only problems with it as a money are temporary due to its immaturity in the market.

Much of the regulatory discussion in Australia has been focused on the question of whether Bitcoin qualifies as money. Different legislation has been interpreted reaching conflicting conclusions. Many of the arguments in favour and against compare the defining features of Bitcoin using existing examples of designated money such as currency issued

---

<sup>18</sup> The original "Satoshi Client" source code is available here: <https://github.com/bitcoin/bitcoin>

<sup>19</sup> Strictly speaking, control of transaction auditing is shared among the "Bitcoin Miners" proportional to their computing power, however this control does not permit them to counterfeit or fiddle the till.

<sup>20</sup> "Antifragile", Nassim Nicholas Taleb, Random House, 2012. <https://en.wikipedia.org/wiki/Antifragile>

by a sovereign nation when interpreting the GST Act and various other legislation. One strategy commonly used is to attempt to determine whether Bitcoin is used primarily in the way that currency is defined and typically intended to be used. While that seems reasonable, there is a problem with this approach.

The question of whether Bitcoin is money has therefore become predicated on “how people are using it”. If people use it to buy things, that’s evidence it is money. If people don’t, but instead they buy and hold it for an investment, this is supposed to be a vote against it being money. Much criticism from economists gets stuck on this question.

So why is this a problem?

There is very little disagreement, even among Bitcoin’s greatest detractors that it is a fantastically capable and disruptive technology, a giant leap forward which will make a great impact on the world. There is also a common understanding that Bitcoin has been deliberately designed to be money by careful study of the desirable properties of a money.

If Bitcoin is a revolutionary technology that is expected to deliver massive value as a money, then we should not be surprised that attracts heavy speculative investment in advance of realising this goal. Bitcoin doesn’t pay dividends so the entire investment thesis - frequently misunderstood as a ponzi scheme - is that there is a great future value when the technology realises its goal as a money, but the catch-22 is that it cannot become an acceptable money until it is first blessed by regulators as such.

Of course it’s not really a catch-22 because a growing number of people are proceeding to use it as money either way, especially online, especially in distressed economies like Argentina’s and especially in more sympathetic jurisdictions. But there is enough speculative investment desperately seeking returns that both causes and results in the infamously volatile exponential early stage growth curve.

In other words, the fact that Bitcoin is a dramatic leap forward in potential as a digital currency makes it seem to be such a good investment that it allegedly disqualifies itself from realising that fundamental purpose - the very purpose that drives the future value.

In my opinion, this means that the disruptive technology aspect should be weighed when determining the true definition of Bitcoin because its very suitability as a better kind of money is expected to force an initial surge in speculation. Foreign exchange markets perform price discovery on currency pairs based ultimately on the relative utility of each currency. In the case where apparent utility is a dramatic rising trend, so would speculators push the price up (at least over timeframes long enough to smooth out pure speculation). This doesn’t detract from the evidence that the currency is money, on the contrary, it’s part of the signal of its suitability as exactly that.

One more practical matter is relevant to the question of Bitcoin as money. According to the legislation, if it is accepted as money by a sovereign nation, this recursively implies that Australia ought to treat it as such. While this is a sensible reaction to the introduction of a

fiat currency, its circular logic is ill-suited for a modern financially- and technology- literate country like Australia when tackling the introduction of a new system with so many fundamental improvements over existing money that it stretches the boundaries of the definition. Allowing our interpretation of the intent of the legislation to become stuck on this is a toxic anachronism.

## The NBN All Over Again

I'm no economist or finance expert. My passion is disruptive technologies that have a democratic potential, like the personal computer, like the internet, like Bitcoin. Let's consider the world where Australia's Osborne computer company didn't go bankrupt in 1985,<sup>21</sup> where instead it thrived on the world stage, where the export success of the Microbee<sup>22, 23</sup> wasn't cut short by the IBM PC and Apple Macintosh, and where we didn't let our country's internet infrastructure lag so far behind our needs that the only way forward was an outscaled and politicised NBN catch-up project. Let's consider that world and its economic and financial impact on 21st Century Australia.

Let's not repeat these mistakes with Bitcoin.

Bitcoin is going to change the world, it's going to change Australia. It's going to change us all. The question is whether we can anticipate that change and embrace it, whether we can lead that change, whether we will drive it or whether we will again be a passenger, trailing behind.

My own plan is to drive that change through Bitcoin and blockchain technology and I would love to do it from Australia.

Sincerely,

Chris Mountford

Sydney, Australia

---

<sup>21</sup> [https://en.wikipedia.org/wiki/Osborne\\_Computer\\_Corporation](https://en.wikipedia.org/wiki/Osborne_Computer_Corporation)

<sup>22</sup> "The Secret Project of Granny Smith", The Age, 12 July 2005

<http://www.theage.com.au/news/next/secret-of-project-granny-smith/2005/07/11/1120934156894.html>

<sup>23</sup> <https://en.wikipedia.org/wiki/MicroBee>