[redacted]

From: Chris Reilly [redacted]
Sent: Tuesday, 5 April 2022 1:37 PM
To: Crypto
Subject: Regulating electronic tulips

Regulating electronic tulips

Executive Summary

This is an exercise in futility and irrelevance .

One could of course inquire as to the objective.

Perhaps the crime of controlling encrypted electrons overseas?

Registering the ownership of all Bitcoins and fractions thereof?

Wait, was this not the country where 50,000+ cash transactions over $10,000 were performed by folks, many of whom were sitting on milk crates stuffing cash into CBA ATMs?.

A more productive exercise would be to recognise some absolute technical realities, some obvious global strategic, commercial and political realities and do something useful instead, to ensure there is a set of global standards for electronic currency (largely based on existing infrastructure) which Australia could adopt.

The predictable outcome otherwise is a 'unique' Australian approach, which will ultimately result in irrelevance of the AUD and a payment network controlled by the likes of Apple, Google and various even more aberrant payment currencies.

The process, the paradigm

The paradigm being applied here is almost universal across anything 'technical', that has the misfortune of acquiring the attention of what passes for 'Government'.

A eclectic mix of 'policy' (typically based on, or more accurately used as the cover, 'vision' attributed to a politician just in case), ideas interpreted by the technically challenged ('I am advised that') and an affection for the next big thing - gimmick (typically sold as the 'future' and an opportunity to be a 'world leader'). The promoters of such fantasy always move on before reality intervenes.

Examples include mobile telephone, the NBN, energy 'policy', submarines, some government payment networks and even aviation electronic infrastructure. $100 billion, a hundred billion there. Soon you have serious 'money'.

"Australian laws will (NOT) trump the laws of mathematics", nor any other 'laws' of the physical universe, which include those applying to cryptography.

Just a Little Detail

For a start it is impossible to prove in a non-quantum mechanical world that a copy of 'information' does not exist. Of itself a basic relevant constraint.

Cryptography is a great intellectual blood sport, albeit on occasion with significant consequences. Some of the nuances are outside the scope of this missive. However the potential to obliterate an electronic nation state are obvious.

Some History

Prior to the establishment of an Electronic Funds Transfer standard (AS2805) things might be described as 'Micky Mouse' in the Land of Oz. The cartel banking industry had established 'Bankcard' with 1 digit allocated to identify the issuing bank and some what arrogantly allocated themselves 1,000 IIN (International Issuer Numbers), which is similar to making up your own number plates.

The prize for idiocy in this space however, goes to the Health Insurance Commission, who invented not only their own numbering scheme, but their own encoding standards, thus ensuring their cards would not be processed by any network based on ISO standards. When asked to justify this, the relevant bureaucrat responded with the statement that the HIC was an "Insurance Scheme" not a payment network.

In both cases paying Standards Australia $10 for copy of the relevant ISO standard might have saved the odd hundred million dollars, but who is counting?

It should also be noted that the response of the cartel banks to the outrage of establishing a national EFT standard was correspondence, some underlined and in BLOCK LETTERS of a less than productive nature.

Due to a lack of a computer science education on the part of the cartel, including of particular relevance game theory, the occasional dispensing of humiliation (Did not finish school? Don't spell cryptography? Too bad you lose.) and the killer move "This is what we are doing at ISO" adult supervision prevailed.

An encore is not looking likely.

BLOCK CHAIN(!)

At the risk of relegating whole aircraft loads of academics attending seances to irrelevance, albeit not before supplying the basis for post doctoral fellowships, cryptographic chaining, is not a original concept.

Indeed it has some established relevance to payment networks, albeit with a aberrant history.

Not surprisingly military system are a tad hierarchical. During the Falklands War an operational difficulty arose. (Someone with the equivalent of the Master Key got shot.) Unfortunately, there are Argentinians who understand English, so the resort to clear comms proved a tad embarrassing and some of the author's mates got engaged in formulating an automated response to this irritating occurrence. This produced a encryption key management scheme, which had a unique key per transmission. However, since the British Standards Institute did not allow grubby entities such as technology suppliers, even defence contractors, to participate in banking standards, which was reserved for senior bankers, one of whom appeared in a Roller at a London ISO meeting, a more lateral approach was required.

The original scheme had a problem, since it was based on random numbers. While in a military environment what happened yesterday was best forgotten (a bit like Canberra), it was considered audit-ability and authentication an essential property for a payment network. Pre-lunch one Saturday morning we stat down to consider the options and I proposed utilising the un-transmitted part of the MAB (Message Authentication Block) as input to a classic one way function, as a key update scheme, thus chain streams of transactions from a card number acceptance device. Objectives included audit-ability, authentication and responding to relevant back and forward tracking threats, as well as devaluing physical compromise to the point of irrelevance. (The active approach of self destruction on tampering might have provided more entertainment, but would have incurred the interest of lawyers.)

This approach was incorporated in the ISO standard (and AS2805.6.2) along with its alternative DUKPT (Derived Unique Key Per Transaction). (I will support yours if you support mine.)

It is worth noting that applying this chaining across multiple transaction sources was considered insane, despite the relative cryptographic elegance of the approach. Of course we were not attempting to invent a new currency, let alone a mining scheme or use the power output of say New Zealand to produce electronic tulips.

Chain your cappuccino purchase or even a new Porsche to a global transaction ledger? Just leave and go to your own planet please.

Law will trump cryptography

Best illustrated by example with the PGP saga.

While a form of asymmetric key encryption was known, its most sensible implementation was developed by three folks: Rivest, Shamir and Adlerman and christened RSA.

The RSA algorithm was indeed patented in the US. Alerted to this and given its obvious relevance of the technology, we documented the algorithm and put it in the EFT the standard. Some months later my long suffering patent attorney called to inform me that he was acting for Public Key Partners, who were asserting ownership of most things related to asymmetric cryptography and maybe I could help. The response was it's a waste of time, while in the US there is a 12 month grace period, in places like Australia public disclosour kills a patent application.

In the US however, there was far more entertainment to be had.

For a start encryption technology was classed as 'munitions' and a controlled export. Indeed there was an attempt to classify a book ("Applied Cryptography") as munitions. The back cover contained a disk with a machine readable copy of some of the printed program source code too. After due legal process (the usual delay) it was concluded the disk was indeed 'munitions', but the same printed text was not.

Since PGP was deemed to be 'munitions' and a prohibited export, the source code was printed and posted off to a saner jurisdiction, where it was scanned and compiled. (Of course, it would have been unlawful to include a disk copy to ensure there were no scanning errors.)

Public Key Partners however had a problem, while it had a US patent, Phil Zimmerman had with the assistance of a mate hiding out in NZ and others, (Its industry practice not to confirm or deny…) had just written a program,

which was being given away. Inventing laws to stop people writing programs might have been an enforcement challenge.

PKP came up with a plan. Produce a program to implement RSA (RSADEF), copyright it and demand every one pay to use it, while refusing to license the patent otherwise. This produced some rather interesting legal analysis citing RICO (That is the Racketeer Influenced and Corrupt Organizations Act), however PKP persisted with a pack of lawyers and assistance from some US government agencies, who have applied the adherence to some rights, somewhat selectively.

After some protracted seances, a settlement was agreed too. A new version of PGP was to be produced, it would incorporate RSADEF, protected by copyright and it would be incomparable with previous versions of PGP. Clearly, the hope was comparability with the now authorized US version would prevail.

A few days after this proud announcement was made, some of us got a e-mail pointing out that if one commented out two lines of PGP source code, recompiled it, then the whole comparability problem went away. Computer nerds 1, lawyers zero.

Want to look really, really stupid? Make laws in this space. Malcolm Turnbull is deemed 'tech savvy' by his admires. (It would be rude to speculate on his own view, since he has declared himself to be a technological agnostic.) However I am sure he would be available to testify on how "Australian Laws will trump the laws of mathematics".

Strategic reality

Australia has a disastrous track record, despite claims to the contrary, in having the rest of the planet adopting unique local practice. A near endless list is again outside the scope of this missive.

Some of it is core cultural.

The orthogonal legal, bureaucratic, political, business, financial and academic elites have clear lines of demarcation. The latter has managed to equate technology to public funded "Research" (All R and no D). That is just as well, since the cartel banking industry is too busy borrowing wholesale OS to fund passive asset price inflation (aka Real Estate), while accumulating the planet's largest per citizen debt, to support quality, productive, value added employment. The arrangement also conveniently avoids all those messy issues associated with actual technology, like organising the money, selling it, making it work and producing a profit, without negating seance attendance.

Mobile? The equivalent of up to 13 sets of gas pipes down some streets per telco! In some cases different transmission modes on the same band, but that's technical. In the beginning of mobile (AMPS) South Korea

started at much the same place. Silly ideas like one coherent technology approach and the idea that everyone's phone should work with every tower, were adopted, albeit in a sane competitive environment? NAH, the Land of Oz adopted a approach based on the 'economic theory' of beach ice cream sellers, which was proudly boasted by one 'economist'.

NBN? Trashing the PSTN, the infrastructure of the telcos was of course insanity. The encore of a set of eclectic transmission technologies, some with fundamental architectural incompatibility, others dependant on rotting paper insulation could be described as criminal. As for making the whole lot dependant on the local power network? Well it just does not work with fires, floods or power failures. Oh and control the power network based on it? (Something about the most basic tenant of control theory.) Suitable for the inevitable requirement of 5G back-haul? Well we would not want to get technical, would we?

Submarines? One can start with the mass density of lead, steel, water, the energy density of batteries and the subtle detail that Australia is a big place. Any analysis resorting to un-trump-able arithmetic and a little physics produces the obvious conclusion that a non-nuclear submarine the size of the French ones are close to useless. A good clue is Energy density of fissile material such as U235 (subs typically use 'weapons' grade) 144,000,000 MJ/Kg. Lead acid 0.14. About a ratio of 1,000,000,000 : 1! Yes the 'laws' of the physical universe will prevail.

Energy? Applying a little of what used to be High School physics, before it all got dumbed down to increase 'participation' and adding a little Quantum Mechanics to this week's energy policy, prompts the verdict "Mindbogglingly stupid". Any sensible analysis starts with citing all manner of folks such as Boltzmann, Planck, Einstein, with late entrants such as Haber and Bosch, to add issues such as the binding energy of N2, NH3 (again properties of the physical universe) to the H2 (2.0) 'vision'. We will 'move forward' as they say in Canberra, or back to the more relevant to crypto.

What NO Laws?

The author was once a guest speaker at the 'Computer and Law Society'. It appears almost entirely composed of lawyers. Even the women were dressed like undertakers. About the only notable thing about this event, was it started with the host expressing the lament that there were no laws about cryptography and lawyers were forced to involve 'experts' rather than rely on 'laws'. Dam! What a ugly precedent. Involving people who understood what they were doing.

Well there are some laws about cryptography and like other laws of the physical universe, are enforced without fear or favour.

They are understood by the likes of the NSA, the FSB, some folks in the PRC, even more than a few non-state actors and even some computer literate children. The reality is that almost all commercial computer software is less than child proof, bits can be domiciled anywhere and fortunately the technology exists to circumvent all manner of state control and surveillance, even if its 'jurisdiction' could be asserted. Thus we have an exercise in futility.

Previous Government initiatives.

Perhaps the most bizarre experience in formulating the Australian EFT standard was a unannounced visitor. Despite being the committees chairman, I usually arrived after the pre-meeting tea and bickies, having a few other issues to deal with, like building out a nation wide network and fabrication some tech that would eventually be the basis of most of the planet's largest EFTPOS networks (including the US, SE Asia etc). We had acquired a mystery attendee (the term guest would have been inappropriate) who had distributed a somewhat bizarre document, claimed to be representing 'the Australian Government', refused to supply his name or identify the author of this missive.

The document implored us to vote down DES (Data Encryption Standard) for the ISO ballot return, because if it were made a standard it would enable "terrorists, criminals and others" to "circumvent lawful surveillance".

The silly detail that such technology was essential to enable all manner of security including EFTPOS, ATMs, bank transfers, not to mention privacy and other deviant behaviour, on the part of the citizenry, was of course deemed irrelevant.

The response from the unwanted, when after the amusement was over, resulting in 13 yes votes was of concern. It was however it was the last we saw of anyone claiming to be from 'Government'.

"**Why is this this so?"**

At this risk of imposing a line of inquiry usually reserved for we physicists, there is a fundamental conclusion which can be drawn from considering the properties of networks, be they the NBN, mobile, power or payment. The core technical architecture is the principal determinant of their utility, 'economics' and control. The architecture is the dominant issue, typically by an order of magnitude or more and 'trumps' the application of ideological based cults such as government ownership, 'the market' and 'competition' policy.

In the case of payment networks it is the cryptographic architecture which ultimately determines the commercial and power relationships.

"*For a successful technology, reality must take precedence over public relations, for nature cannot be fooled".* Richard Feynman

"*The more often a stupidity is repeated, the more it gets the appearance of wisdom.*" Voltaire

BOTTOM LINE

“Regulating” this space is technological masturbation.

Establishing a global technical framework - architecture and even some appropriate technology just might save the likes of Australia from irrelevance since one could consider the definition of a nation state as printing your own money and controlling its payments system.

Would someone pass the electronic tulips please, but don’t tell anyone.

A one line summary – perspective:

Great country, pity about the management.

The author of this missive

Founding chairman of the EFT Standard committee.

Founding chairman of the security technology standards committee. (crypto stuff)

A member of the relevant ISO committees, which wrote the global rules relating to such issues as card numbed transaction security.

Joint founder and group CEO of the AUSTNET group (taken from a start up to the dominant EFT network before being flogged off to some Americans) and chairman of its US subsidiary.

Has been granted (US) patents in areas such as telecommunication and cryptography technology.

Spent a decade working for a US corporation whose clients included the some of the relevant.

A year zero computer science graduate with a major in Physics too. Also one of 6 chosen from 4 Universities for the country’s first computer science honours program. Even did a post grad course in solar Energy Engineering , for no good reason.

Other crimes include working on the nations first and the planet's second computerised message switch and heading up a computer project essential to the core fabric of Australian society (The Victorian TAB) at the age of 23.

In addition, to being responsible for the design and implementation of some of the planet's larger networks, he also organised a billion dollar plan to assault mobile telephony, with the support of the industries more globally credible entities. When the spectrum licence prices in the auction got too dangerous and it became obvious others had done their financial models on another planet, the effort was morphed into a profitable spectrum speculation exercise. Subsequent relevant amusements include noting that the 'successful' bidder lost something north of a billion dollars, with the ultimate contribution being working over the wreckage of one.tel at the behest of Lucent's appointed receiver for the network hardware.

The place is a near endless source of amusement. Sanity however can be found in those who understand that the local equivalent of "Yes Minister" (UTOPIA) is not a documentary, but a series of training videos.

--

Chris Reilly [redacted]