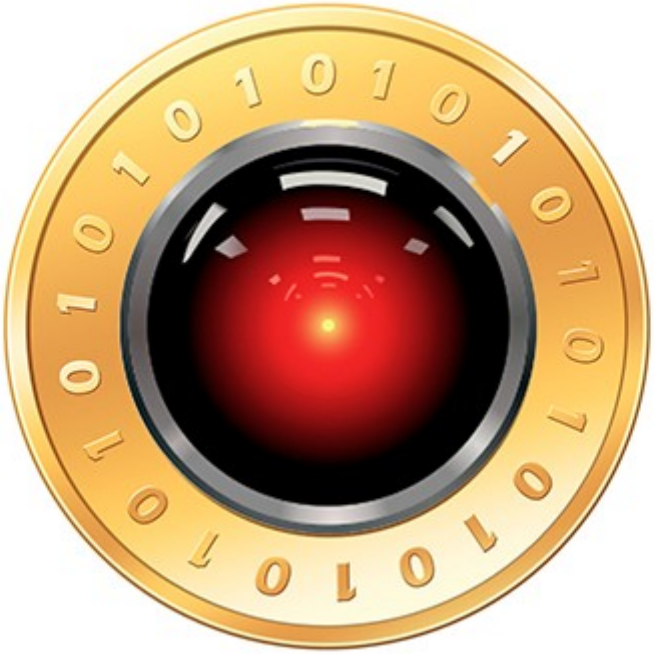

Cypherpunks, Bitcoin & the Myth of Satoshi Nakamoto

Posted by: cybersalon in Writing September 5, 2013 25 Comments 45,599 Views

Introduction

As a movement, Cypherpunk is more nuanced, more serious and more focused than Cyberpunk. Like all good punk movements, Cypherpunk is radical by design and fanatical in its end goal of disrupting the status-quo. If we couldn't see Cypherpunk clearly before it was because books like Cryptonomicon were not as accessible as the pulpy and instantly attractive Neuromancer. Cypherpunk is concerned solely with hidden meaning, secrets and power that can be wielded out of sight from governments and spooks. It is embodied by discrete arrays of public/private key pairs. It is a science that values discretion and privacy above all else, and as such it champions our most closely held secrets and beliefs.

Cyberpunk by contrast was typified by Jaron Lanier's clunky Virtual Reality: pixelated polygon aesthetics from the 1990s and William Gibson's dystopian sprawl culture, but until now, we couldn't really understand Cypherpunk's issues as a culture, because we couldn't imagine what Google would to do us or to our businesses. We didn't know what 'big data' was, or how social networks would assimilate our friends, acquaintances and close family members into one amorphous communicative membrane. Neither could we envision how peer-to-peer networks might threaten Hollywood and Wall Street.

When Neuromancer was originally published in 1982 we couldn't even get our heads around what a web browser was. Cyberpunk in the 1990s was all techno music and wild hair, squat parties and bad video art. Cypherpunk, by contrast was RSA, PGP and the NSA. Now, it's BTC, GCHQ, PRISM, SHA-256, TEMPORA and RAGTIME-P (Stellar Wind). It's a world full of acronyms and codes, impenetrable to all but the most cynical, distrustful, and political of minds.

In literature, those who are lost to history are occasionally referred to as 'ciphers'. It's a peculiar use of the word because it implies that the person is a lost word or code in the logos, not understood in

their time. The root of the word is from the Arabic ‘sifr’ meaning zero, empty; so Satoshi Nakamoto, the inventor of Bitcoin is the historical “cipher-punk” par excellence.
This meaning of ‘cipher’ does not apply to our historical luminaries. Rather than benefiting from an absolute right to privacy, luminaries belong uncomfortably to the public domain where they suffer an element of transparency. This is a crucial point to understand because the Cypherpunks do not wish fame, exposure or recognition. Their philosophy can be summed up simply by Assange’s essential maxim: ‘Privacy for the weak, transparency for the powerful’.

The Cypherpunks

The Cypherpunks began properly in 1992 when Tim May, Eric Hughes and John Gilmore, started the Cypherpunks’ mailing list. But Jim Bell, David Chaum, Phil Zimmerman, Julian Assange, Adam Back, Wei-Dai and Hal Finney are just a few of the ciphers on the mailing list who are just now becoming luminaries, because they’ve all contributed something so uniquely valuable to us through their efforts to protect our privacy in the new information economy, particularly against the encroaching financial surveillance complex (typified by FATCA).
Other names, like Tim-Berners Lee, John Perry Barlow and Nick Szabo also feature in this essay, as ‘Cypherpunks by proxy’ because of their contributions and their philosophy.
Tim May’s seminal 1992 document ‘The Crypto-Anarchist Manifesto‘ states:
“Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity of the other. Interactions over networks will be untraceable, …with nearly perfect assurance against any tampering. Reputations will be of central importance, far more important in dealings than even the credit ratings of today. These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation.”
In 1993 Eric Hughes wrote his original statement on the mission and goal of the Cypherpunks called ‘ A Cypherpunk’s Manifesto‘, in which he says:
“Cypherpunks are dedicated to building anonymous systems… Privacy is necessary for an open society in the electronic age… We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy…We must defend our own privacy if we expect to have any. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money”.
May also went on to write ’The Cyphernomicon‘ which was later echoed by Neal Stevenson’s historical fiction entitled “Cryptonomicon” in which “[a] narrative is set in the late 1990s with characters […] employing cryptologic, telecom and computer technology to build an underground data haven […]. Their goal is to facilitate anonymous Internet banking using electronic money and (later) digital gold currency”.
David Chaum was the most notable early champion of the Cypherpunks’ goal of realising a digital currency in ‘Digicash’. In some ways, Digicash was a spectacular failure, sometimes unfairly attributed to Chaum’s greed; but in the best ways, its failure was instructive because it demonstrated perfectly that a privately issued digital currency could not survive the legal system’s onslaught of regulations (AML and KYC in particular). Exactly the same story has been seen being played out again and again, with e-gold’s failure, whose CEO Douglas Jackson narrowly avoided being sent to jail, and more recently with the Liberty Reserve Dollar and Arthur Budovsky‘s arrest.

Bitcoin's Sovereignty

The fundamental difference between these private currency operations and Bitcoin is that the former units of exchange are issued by private corporations and are backed by something, usually paper or real gold, or silver. As such they suffer from a fatal flaw: that whoever is issuing the unit of exchange has a monopoly control over and can enrich themselves at the expense of the other people using the currency.
Whilst the dollar is backed mostly by political force (the threat of forgery protected by imprisonment or violence), legitimate banks can manipulate the international money markets by devaluing their currency. The rules that apply to banks, also apply to the privately issued currencies like those mentioned above, and they must all be highly regulated. They must do due diligence on their customers and follow rules like: 'Know Your Customer' where they must be able to verify the true identity of their clients, and they must keep records of what their customers are buying and selling with their digital tokens.

Recently we've been informed about the US government's use of FISA, the 'Foreign Intelligence Surveillance Act' of 1978 (amended much since 9/11) which effectively enables the US government to make requests for information about a private company's data. In the UK, it's RIPA (Regulation of Investigatory Powers 2000) that enables this process. Using FISA or RIPA, our governments can lay claim to the most sensitive of private data, from meta-data about calls and communication to the KYC databases.
Private companies like the 'Liberty Reserve', who issue anonymous tokens backed by silver have to keep records of the transactions that their customers are making. If they refuse to comply with the governments requests for detailed information, they can be prosecuted, and of course, their 'anonymous' systems are used extensively by criminals of all flavours: from money launderers, child pornographers, to drugs and arms dealers.
It's actually a great catch for the British and American intelligence agencies to be able to capture that information. Bitcoin differs because it belongs absolutely to the public domain. It is issued by relatively public (albeit anonymous) individuals, it costs real energy and resources to create, and its transparency is facilitated by the use of a publicly distributed peer to peer ledger that everyone can easily access. There is no corporation that keeps records of the names of transactors, and there is no CEO to prosecute so no government entity can exert absolute control over it through regulation or legislation, whether by FISA or RIPA, provided that the user enters the system and uses the bitcoins in an anonymous way.
Understandably, governments don't like this, and they're desperately trying to find ways to regulate (or at least classify) it. In April 2013 a study from the university of Chicago released a document which concerned how the IMF could potentially address the threat that Bitcoin now poses to the global economy in its capacity to launch speculative attacks on national currencies. The technicality is that they (the IMF) cannot buy Bitcoins because it is a stateless currency, and according to their articles of association they can only hold reserves of state-backed currencies. This is a dilemma for the IMF, and puts them directly at odds with the Cypherpunks' politics, which is precisely the point.
Perhaps John Perry Barlow's words, keeping with the spirit of independence akin to the founding fathers of the US, put it best in his now famous 'Declaration of the Independence of Cyberspace' when he stated:
"Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather…
Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions."
For those wary of Bitcoin's pedigree, it may comfort them to know that it emerged directly from a culture of programmers who champion open-source software (also known as free software) like Sir

Tim-Berners Lee, who invented the World Wide Web. The ‘shadowy hacker’ label that is sometimes ascribed to Satoshi Nakamoto is fair in some ways because that’s the way he intended it. Satoshi thus embodies all the things that the original Cypherpunks were trying so hard to impress upon us: our fundamental right to privacy. It is Bitcoin’s capacity to protect some aspects of our privacy from GCHQ and the NSA that makes it valuable – to a degree. But it’s more than that. Bitcoin has high utility, and gains some value from its scarcity, but more from its inherently democratic and ethical design.

So whilst Bitcoin may have been conjured from the dark space that bore markets like the Silk Road, Bitcoin is a purist and egalitarian creation by nature of its architecture and implementation. It is not monopoly controlled, it is not a privately backed currency, it is an emergent currency, backed by our increasing understanding of peer to peer networks, and complex mathematics (specifically one-way functions as applied to large prime numbers). It incorporates all the best elements of the crypto-voodoo that the Cypherpunks were so enamoured with, with the crucial proviso that all the cryptography used in its construction belongs firmly in the public domain and is therefore open to peer-review.

This is of critical importance because it prevents agencies like the NSA or GCHQ being able to insert their own private ‘back doors’ into the algorithms, meaning that transactions can be made anonymously and securely, remaining purely within the domain of the transactors; and this is precisely what is at stake with the current revelations about GCHQ’s TEMPORA program, the NSA’s PRISM program, and their less well known but equally terrifying RAGTIME-P program; capable of mapping an entire person’s life (since 2001) by domains, social, financial and communicative into three dimensions, along a historical time-line.

The technologies that the Cypherpunks have developed over the years; technologies such as TOR, Freenet; I2P, and Bitcoin, lie firmly within an open source ideological framework, and have effectively become tools to defend privacy, against invasive and potentially abusive governments, and ‘Open Source’ is fast becoming a religion in its own right. In a sense, it has philosophical ties to peer-reviewed science: it is open to criticism, and it is therefore open to innovation and advancement.

To make things clearer, the cryptographic roots of Bitcoin stem from the legacy of Ron Rivest, Adi Shamir and Leonard Adelman who pioneered the RSA algorithm (the first commercially available cryptographic algorithm) in 1977, and Whitfield Diffie and Marty Hellman’s ingenious invention of ‘Public Private Key Cryptography‘ in 1976, a method now used in everything from PGP email (now more commonly used in GnuPG) to the Bitcoin network protocol. Both of these cryptographic innovations were closely watched by NSA who initially classified them as threats to national security and therefore as munitions, but they eventually gave up trying to contain them in the late 1990s and early 2000s when both RSA and the Diffie-Hellman-Merkle key exchange were finally and terminally released into the public domain.

It was these two key innovations, and the development of the peer-to-peer network by Shawn Fanning and Shaun Parker with Napster, that allowed Bitcoin to become a reality. They allowed the publicly distributed transaction ledger to be shared amongst a network of honest participants who could all continuously check that the ledger did not include any double spending and had not been tampered with.

There was however, one final, and brilliant solution to the problem of ‘double spending’ which made the whole system viable. Double spending was a problem that had plagued digital cash since its inception: the solution came in the form of Hal Finney’s concept of ‘Reusable Proofs of Work’ based on Adam Back’s invention in 1997 of Hashcash; originally a “proof-of-work system designed to limit email spam and denial of service attacks”, in combination with Dahlia Malkhi and Michael Reiter’s academic work on ‘Byzantine Quorum Systems’.

RPOWs (as they came to be known) really came into their own and did away entirely with the need for a central time stamping server that could be compromised by crooks wanting to re-spend their digital cash over and over again. Satoshi explained how RPOW’s could be used to solve the Byzantine General’s Problem, a problem in general computing that demonstrates through game

theory how a group of potential co-operators can come to the best consensus even with the possibility of having defectors in their midst. His explanation for how proof of work can be used to eliminate the need for a trusted third party is here.
Hal Finney responded to Satoshi on his original posting of the Bitcoin whitepaper on the cryptography mailing list at Metzdowd; he was also a keen observer of Wei-Dai's original post on /b/money which begins:
"I am fascinated by Tim May's crypto-anarchy. Unlike the communities traditionally associated with the word "anarchy", in a crypto-anarchy the government is not temporarily destroyed but permanently forbidden and permanently unnecessary. It's a community where the threat of violence is impotent because violence is impossible, and violence is impossible because its participants cannot be linked to their true names or physical locations."
Dai goes on to outline the original idea for Bitcoin which is then fleshed out fully by Nick Szabo in his article 'Bitgold', published in 1995 and then republished again on his blog 'Unenumerated – Bit Gold' in 2008 where he fully articulates Dai's idea. It is Szabo's writings that are crucial to the intellectual development of Bitcoin and digital property rights in general.

(If you enjoy this article, or find it useful for your research, please consider donating BTC to 1AU8WhY6RHRYcr7heCNfj5YGHTELFkBQNP Thanks!)

Satoshi Nakamoto

Satoshi Nakamoto is in effect then, a kind of amalgam of the cypherpunks' fusion of characters, with some of them, like #Chaum #Dai, #Finney, #Reiter, #Back and #Szabo, perhaps more crucial to Bitcoin's development than others, but Satoshi is an important historical cipher precisely because he is mythical, and rather than being forgotten, Satoshi can be considered a neo-saintly archetype for the digital age, conjured as if from a William Gibson novel. Like Neo from the Matrix, he is from a place where "government is … permanently forbidden and permanently unnecessary", a figure who owes something to all the founding fathers of Cyberspace.
As ours is a distinctly post-religious culture, like V from 'V for Vendetta', Satoshi emerges from the darkness of the digital underground to lead the masses in a brave new world against the banks, oligarchs and multinationals; all who benefit from our ignorance about the nature of money, our powerlessness over entrenched state monopolies and our obedience to the collusion of government and big-business.
Let's say then, that Satoshi Nakamoto is a convenient fiction and that it behooves us as a culture to construct and mythologise him as a figurehead around whom a loose network of global hackers and freedom fighters can rally. Anonymous, Occupy, Wikileaks, Bradley Manning, Julian Assange and Edward Snowden, abhor the surveillance state and say they want to see an end to corruption. They are whistleblowers who are peaceful revolutionaries by nature, they are intellectuals and pragmatists, who believe in non-violence, and who are true children of the internet age. The government may label them as dissidents, but it's more appropriate to class them as heroes. They wish to challenge the old order and institute a fairer, more egalitarian society, a world where education is freely distributed and available to all, and where privacy is a right not a privilege.
To this end, and for those who believe in a fairer world: we're all Satoshi. #wereallsatoshi
The key is, how can we apply Bitcoin to ethical markets rather than black markets? How can we implement it ethically to make a fairer and better world? Because the potential to redress the balance of wealth, to incentivise distributed computing problems like "Folding@Home', to cure Cancer and Lou Gehrig's disease using this technology is huge. It may not be something we can fully appreciate in our lifetime: but the reason I'm so passionate about it is that it may also be a tool

by which to confront ‘The Monopoly Empire’ of profit and greed as we’ve known it for centuries, spur development in the poorest countries, and help those who need it most.

@richardboase
richard@richardboase.com

Thanks for reading this article, if you learned something new or you would like to syndicate, reference or link to it, please consider donating some BTC to 1AU8WhY6RHRYcr7heCNfj5YGHTELFkBQNP Thanks!