HEAT EXCHANGES

FINN BRUNTON

Hot Bits

This is a story about two beautiful abstract entities awkwardly struggling to exist in the constraints of the actual universe. These entities are called *money* and *the wire.* Like Gnostic forces, they are the crude form of what they could be, haunted by their other forms: perfect information, permanent value, lossless transmission. You've almost certainly already encountered them today before reading this. What follows is a history of how they met in the genesis of cryptocurrencies, and what they can tell us about how computers compute and how money holds value – about how they draw strength and solidity precisely from their friction-laden failure to live up to our models.

Starting with the wire: singular, because it is as free of individual peculiarities and distinguishing characteristics as one Platonic sphere from another, as exact as an axiom. The engineer and scientist Danny Hillis, part of the team that produced the massively parallel supercomputer the Connection Machine, describes the wire as a 'costless and volumeless idealized connection'.[1] You put data into one end of the wire, and the data appears in one or many other places. It is instantaneous, it is cheap, it is tiny, and it dissipates no power. It can be ordered from the same catalog as the frictionless boards and massless pulleys of introductory physics. It is fantastically useful for thinking and design, but sadly it must share our universe with us. Wire transmission can therefore be as good as instantaneous – but it will still take a bit more than three nanoseconds under ideal conditions for a signal to travel a meter. Factor in less-than-ideal media, and handoffs, interchanges, and switching systems, and you can produce one of the earliest and still most beautiful 'phone phreak' hacks: routing a call from relay to relay around the planet all the way back to another line in the same room. Two phones sit on a table, and when you speak into one your voice comes out of the other after a brief delay, making the Earth into your Echoplex effect pedal.[2] The wire is instant, but wires take time, however little. Wires cost, however cheap, and occupy space, and they must dissipate power – which means generating heat.

As a practical matter, the work of computation is the work of managing heat. The history of computing is also a history of air conditioning and temperature control. Start when you like: Charles Babbage discovered that the gears of his programmable, calculating Difference Engine generated enough friction to challenge the limits of Victorian-era

[1] William Daniel Hillis, *The Connection Machine,* PhD diss., Massachusetts Institute of Technology, Cambridge MA, 1985.

[2] Ron Rosenbaum, 'Secrets of the Little Blue Box', *Esquire Magazine,* October 1971.

tooling technology, in the effort to avoid 'all possibility of derangement in the machinery',[3] and therefore of the results it produced. In early electrical computers, the challenge of keeping the results of a given computation in working memory – available to be fed back into an ongoing process – resulted in the marvelously improbable solution of *delay line memory*, which used the propagation of a circulating wave as the equivalent of repeating a phone number over and over to yourself as you hunt for a pen with which to write it down. Of course, for this to work, you had to know reliably how long it would take a wave you've sent out to come back, which means having exactly the right fluid at exactly the right temperature. Getting things in time, for computing, means having them in space, with a clear picture of the speed of sound: therefore tubes filled with glittering mercury were wrapped in coils keeping them at 40 degrees centigrade, storing hot and noisy bits. (UNIVAC I had pulses of sound set aside to confirm that travel at the right speed was happening, to correct the temperature accordingly – a thermostat that used time as a picture of space, which was in turn an index of heat.[4]) 'Noisy bits', literally: many sources of inaccuracy or noise, like reflections off the interior of the tube, had to be accounted for, and the delay line pipes themselves were nice and loud, a rattling click track for the operation of an algorithm.

Over the years the source of the noise shifts from discrete to continuous, from the distinct waves rolling through the hot mercury to the roar of the air conditioning, the sound of computational work being done. Moving current through a conductor results in Joule heating, collisions between electrons and atomic ions giving off kinetic energy – an amount of heat proportional to the square of the current. Illustrations of this abound, most obviously in the warm glow of an incandescent light bulb, whose filament shines with resistance to the current passing through it. Heat pours out of the digital machines built with vacuum tubes, akin to light bulbs, whose on-ness or off-ness holds the state of a computation; EDVAC had more than 3,000 tubes, and needed an air conditioner that consumed about half its power.[5] In the Princeton summers, attending to the ENIAC machine – with its special refrigeration units because it 'ran very hot',[6] constantly failing – was like working in a ship's furnace, and the gunk messing up the IBM punch cards was tar that had melted and dripped down from the roof. Air was blasted over the mechanism at 4,500 cubic feet a minute and the humid atmosphere of New Jersey iced over the coils.[7]

'Big iron', the massive mainframe machines that stood apart from early personal computing – stood, indeed, like plinths or menhirs, full of complex engineering and design choices to maximize processing power – had to be embedded in a *thermal architecture* capable of sustaining their operation. The IBM 704 (still with vacuum tubes, now featuring floating point operations) was the computer used for the voice synthesis experiments that inspired the demise of HAL 9000 in Kubrick's *2001: A Space Odys-*

[3] Unsigned obituary, 'Charles Babbage, Philosopher', *Van Nostrand's Engineering Magazine,* October 1871.

[4] Sperry Rand Co., *UNIVAC I Maintenance Manual For Use With UNIVAC I Central Computer,* sections 1-75 to 1-99, New York: Sperry Rand Corporation, 1956.

[5] M.D. Godfrey and D.F. Hendry, 'The Computer as von Neumann Planned It', *IEEE Annals in the History of Computing* 15.1 (1993): 13.

[6] Charles Schrader, *History of Operations Research in the United States Army, Vol. I 1942-1962,* Washington D.C.: CMH Pub 70-102-1, 2006.

[7] George Dyson, *Turing's Cathedral: The Origins of the Digital Universe,* New York: Vintage, 2012.

sey, whose melancholy song is carried on in eerie quiet, presumably because HAL could vent waste heat to space.[8] The actual 704 needed an air conditioning apparatus rumbling away: the machine installed at RAND had an entire under-floor plenum devoted to pumping cold air up through the cabinets, over the tubes.[9] The 704 at MIT had air conditioning failure alarms, so engineers could come sprinting in, like emergency room doctors in a TV drama, to yank panels off the box and keep the patient from overheating.[10]

As the transistor and the integrated circuit condense these room-sized architectures into the thumbnails and postage stamps of chips, microscopically etched with photolithography, this problem becomes more extreme: the chips now have to get heat out of themselves, out of their envelopes of ceramic and plastic, and then the machine that encloses them must in turn do something with it. Moore's Law means the number of transistors that can fit on a chip doubles every eighteen months, and each doubling is another threshold of power dissipation to be crossed. The first Cray – a supercomputer for scientific projects that required processing huge volumes of data (Las Alamos National Laboratory got the test machine with serial number 001), developed by a team led by Seymour Cray – was a masterpiece of heat management. It used high-speed integrated circuits set back-to-back on sheets of copper mounted on tubes of Freon, the now-restricted refrigerant gas from DuPont, working like the coils of an air conditioner.[11] The center of each 'module', the stack of circuit boards, could never get above 65°C, which meant the plates, bars, and refrigerant system were connected to two twenty-ton compressors outside the computer room. Construction delays rested on getting the pumping system right; all the patents for the original Cray-1 were for innovations in cooling. The cool, ice blue, virtual world of *Tron* – parts of which were rendered on a Cray-1 – rested on a vast cloud of searing hot air.

This heat became part of the everyday practice of personal computing, signaled by the moment you hit the key command to save a Photoshop file and the program lurches, hangs, and suddenly the fans kick on. PC gamers running high-end graphics began building hot-rod boxes with fans like turbines, the parts assembled inside refrigerators with the gleaming edges of the components softened by the fog of condensation on the exterior glass. Gamers wanting laptops can buy or build custom machines, like Christian Sandvig's *Sager Notebook*, with a motherboard plated in copper. When the system switches to the powerful desktop graphics card, '[t]here is a sound like a jet engine starting up and the person sitting to my left is from then on continuously bathed in a stream of hot air'.[12] Or, like the sociologist danah boyd, people needing a lot of computational work in laptop form could burn their thighs and hope for a firmware upgrade.[13]

[8] Geeta Dayal, 'Max Mathews (1926-2011)', *Frieze,* May 2011, http://blog.frieze.com/max-mathews/.

[9] Willis H. Ware et al., *RAND and the Information Evolution: A History in Essays and Vignettes,* Santa Monica: RAND, 2008.

[10] Steven Levy, *Hackers: Heroes of the Computer Revolution,* Sebastopol: O'Reilly Press, 2010.

[11] James S. Kolodzey, 'CRAY-1 Computer Technology', *IEEE Transactions on Components, Hybrids, and Manufacturing Technology* 4.2 (June, 1981).

[12] Personal communication with the author.

[13] danah boyd, 'Blotchy Burns on My Legs from my Macbook', *Zephoria*, 9 September 2007, http://www.zephoria.org/thoughts/archives/2007/09/09/blotchy_burns_o.html.

The heat of computation is now, for many, less of a daily experience than before, but that isn't because the heat is a solved problem and the bits move without resistance. More and more of the heavy computational lifting is now exported to the cloud. The phones and tablets and netbooks can be as light as they are, and keep what battery life they have, by relying on the serious work being done elsewhere, in places like Sweden, Finland, and the higher latitudes of the Pacific Northwest, where massive server farms can be chilled by wintry air and geothermal power.[14] Whether under the aurora or in a New York City summer in one of the AT&T buildings downtown, the server racks are arranged within their own thermal architecture of hot and cool aisles, a structure that ensures the steady flow of air, the highest possible cubic-feet-per-minute throughput, rushing like a river carrying heat away from the venting machines.[15] Behind the chain-link, under the trunks of tagged and zip-tied ethernet cables, layouts of flowing air and carefully chosen temperature gradients have created an accidental version of Yves Klein's 'air architecture', in constant motion.

One of Seymour Cray's other patents concerns the use of a liquid from 3M called Fluorinert for immersion-cooling circuit boards: 'Unfortunately, that theoretically possible high density cannot be achieved in practice unless a very considerable amount of heat generated by such a high density assemblage of circuits can be successfully removed.'[16] In Hong Kong just such a set-up exists, with an inert liquid (one in which electricity does not conduct, making it safe for computer components) boiling in tanks filled with ranked circuit boards. But the chips aren't cranking through climate models or rendering polygons for cinematic airships. They're solving a set of arbitrary challenges to produce hashes of data – that is, they're mining Bitcoin.[17]

Making Money Money

'Superdollars', said a Europol anti-counterfeiting officer, 'are just U.S. dollars not made by the U.S. government'.[18] He was speaking of the counterfeit U.S. hundred called the Supernote, believed to originate from North Korea (likely cranked out on the excellent currency presses inherited from East Germany after the fall of Berlin Wall, where they'd served to fund the activities of spies in need of ready foreign currency). The Supernote is a beautiful production. Indeed, one of the very few ways that one run of the notes could be distinguished from Federal Reserve issue was that a few of the minute scenes were *too* perfectly rendered, with lines crisper and clearer than they ought to be, though even that was only visible to the best-trained currency specialists looking through loupes.[19] It cuts to the heart of the strangeness of currency, to the multi-layered problem of trust. We trust that the notes we pass are real – to knowingly pass a counterfeit note is a crime – and that the body issuing the notes will not print too much money, and they will retain

[14] Nicole Starosielski, 'Digital Media: Hot or Cool?', *Flow* 15.5 (January, 2012).

[15] Rongliang Zhou et al., 'Modeling and Control for Cooling Management of Data Centers with Hot Aisle Containment', *Proceedings of the ASME 2011 International Mechanical Engineering Congress & Exposition,* November 2011.

[16] Seymour Cray, 'U.S. Patent No. 4,590,538: Immersion Cooled High Density Electronic Assembly', United States Patent Office, 18 November 1982.

[17] Xiaogang Cao, 'Visit of ASICMINER's Immersion Cooling Mining Facility', *Bitcoin Forum,* 25 November 2013, https://bitcointalk.org/index.php?topic=346134.0.

[18] David Wolman, *The End of Money: Counterfeiters, Preachers, Techies, Dreamers – And the Coming Cashless Society,* New York: Da Capo, 2012.

[19] Stephen Mihm, 'No Ordinary Counterfeit', *New York Times Magazine,* 23 July 2006.

their value more generally. We need confidence, and the notes must reflect this through a combination of security technologies and public assurance.

Thus currency is pulled from circulation when it starts looking shabby, and each note is embedded in networks of material scarcity and complexity that will enable it to meet the criteria of mints and central banks: that it be easy to produce and easy to verify, and very difficult to reproduce or to fake. There is a certain structural similarity here that will echo for those familiar with the P versus NP problem in computer science. There are classes of problems for which a computer can quickly determine whether a solution is valid, but which will take a long time for the computer to solve – so it can swiftly verify that a private key is the right solution to the problem that deciphers the encrypted message, but it would take epochs of time to arrive at the right solution itself. All the labor of currency work, with the reactive inks, security threads and special fibers, watermarks and holograms, is the work of making it so one institution can produce units by the millions, enough to keep not just a country but the international movement of trade flush with ready money, while another institution would find it difficult to produce a single such unit.

Of course, what makes money money is an enormously complex, abstract question that touches, at its deepest, on the foundations of human community and communication itself: on language, shared understanding, trust and everything contained in the concept of *exchange.* We could tell stories about cigarettes or beautiful snow-white slabs of salt on the backs of Bactrian camels on the Silk Road; we could cite trading networks of beads made from the pearl teeth of red deer around the Mediterranean basin about 46,000 years ago, or *World of Warcraft* gold.[20] But, for purposes of this essay, let's keep it simple. Money is what passes for money – that is, what you can pass in exchange for other things, and much, but not all, of what passes is a matter of sovereign decision. The sovereign, whether a monarch with a crown or the authority vested in a central bank by a representative government, has the right of mint and issue. They can do things like, in the case of the United States, make it law that a debt you owe can be paid by you in U.S. Dollars – your creditor cannot insist you pay it in euros, gold, or cocoa beans. They can police who is allowed to produce money that passes, and under what conditions. This work is obviously, trivially, about authority, but it is also about trust and confidence.

'The same ignorance makes me so bold as to absolutely deny the truth of the various ghost stories', this is Kant speaking, in his small book on the visionary mystic Emanuel Swedenborg, 'and yet with the common, although queer, reservation that while I deny any one of them, still I have a certain faith in the whole of them taken together'.[21] I've started taking pictures of the little signs I see up at coffee shops, movie theaters, grocery stores and other spots that do a lot of business in cash, announcing that they no longer accept hundred, and in some cases fifty, dollar bills. These often hang in the foreground of the signs behind the register that itemize the traits identifying counterfeits and giving hotline numbers. It is easy for us to distrust any particular note while

[20] Daniel Lord Smail, Mary C. Stiner, and Timothy Earle, 'Goods', *Deep History: The Architecture of Past and Present,* Oakland: University of California Press, 2012, pp. 219-240.

[21] Immanuel Kant, *Dreams of Spirit-Seer by Immanuel Kant and Other Related Writings,* trans. John Manolesco, New York: Vantage Press, 1969.

still believing in ‘the whole of them taken together’. The question of when that general trust begins to shift is a fascinating one – consider Wesley Weber, whose counterfeiting of the Canadian hundred-dollar note was sufficiently high volume that it made Canadian hundreds effectively unspendable in many large cities until the new issue. (In this context we can also look at Operation Bernhard, the Nazi project to counterfeit Bank of England notes to finance espionage and imports, and to drop in huge volumes from the air over the U.K. to crash the economy through inflation and insecurity in the currency.) There are larger reasons for the trust in currency generally, from the participation in imagined communities to the simple fact of ‘passing current’ – consensus understanding within a community that something accepted for payment here can be redeemed there – but part of it is technological: the technology of trust as embedded in currency itself.

A moneyer with Suns of Liberty Mint in the United States described perhaps the simplest form of this experience of trust to me: ‘Silver is silver, and the weight is the weight.’[22] He captures a whole world – one lost to most of us now – of monetary experience built around the intimate empiricism of metal: biting into a coin, weighing it in a scale or the palm of a hand, striking it to hear the chime. Far more elaborate versions of this process are still performed at events like the Trial of the Pyx at the Royal Mint (or, to be more precise, at Goldsmith’s Hall in London), where a gathering of experts assay the coin issued by the Mint as they have for several centuries. However, even for non-experts, metallic currency contains mechanisms making it possible to do the work of evaluation – like ‘milling’ or ‘reeding’, the fine, narrow-set hatching on the edges of coins. This makes it easy to spot, or to feel with a fingertip, if a coin has been ‘clipped’, part of its precious metal content shaved away with a sharp knife so the coin can be spent for face value while the clipper can keep a bit of the bullion value.

Paper money takes these challenges much further: we recognize real notes by feel, by reactions under ultraviolet light or to a special pen (which doesn’t actually identify valid bills, but rather reacts to the properties of toner used in color copiers and printers), by optical tricks (ink that modulates green-black in color when turned) and holograms, by size, by texture (whether the delicate, slubby feel of intaglio printing on cotton, or the crisp, glossy quality of plasticine notes), by special fibers like security threads and watermarks. Even so, counterfeit notes are surprisingly easy to pass. The canonical reference for prop money produced for film, television, and theater captures the problem.[23] The bills have to look good on camera – stuffed in a briefcase, flashed by a villain, and so on – but they are rarely in close-up, so the production facilities that produce them have found many ways to make it clear that these are not real notes. They will have fake political figures, gibberish text, misspelled words, even warnings like ‘For Motion Picture Use Only’ (albeit in the appropriate typeface and color for the bill, to keep it from being noticeable to an audience). Even so, prop notes have been spent. ‘If it’s green and says 20 on it,’ said a Secret Service agent policing prop money production, ‘somebody will take it.’[24]

[22] Personal communication with author.

[23] Fred Reed, *Show Me the Money!: The Standard Catalog of Motion Picture, Television, Stage and Advertising Prop Money,* Jefferson, NC: McFarland, 2005.

[24] Richard Fausset and Andrew Blankstein, ‘Films’ Fake Cash Can’t Look Too Real’, *Los Angeles Times,* 6 June 2001.

The problem of electronic digitization and duplication means that currency also now exists not simply as notes with particular characteristics, but as a set of international agreements embedded in software and firmware on color photocopiers, printers, and graphics editing systems like Photoshop. The EURion Constellation is a pattern of dots whose arrangement triggers currency recognition systems built into copiers, which will then be unable to reproduce the item.[25] (If you are holding the Mexican 20 peso note, it's the small yellow circles in the band by Benito Juárez's head; on the 10 euro note they're in the visual echoes of the arch; the American $ 20 dollar hides them in small yellow '20's.) This is a fairly obvious ploy, and the properties that make a banknote distinguishable so Photoshop will not allow it to be scanned and manipulated are still being researched.[26] To manage the problem of counterfeiting even physical currency must function digitally, within a political framework of agreements and common standards, to keep its object-ness from falling into question.

Of course, on the flip-side of the question of confidence and trust is that of the behavior of the *legitimate* producers of money. Will they print too much? Will they print too little? As the cultural historian Bernd Widdig has identified, one of the crucial symbols of the experience of Weimar hyperinflation was the sheer volume of paper money: the walls lined with stacks of bound bundles of notes being tallied by clerks, the devalued notes being sold by weight for fuel.[27] The crisis of legitimacy – of confidence in the issue of new money – was expressed in the properties of the notes themselves. Their ink was sometimes still wet when they were rushed out to banks and businesses, a physical index of the scramble to stay ahead of the inflationary spiral; extra zeroes were stamped onto notes; under the worst conditions, some were only printed on one side. The weight, the mass of money was a direct concrete expression of how valueless it was: one would no more gather it than you would armfuls of wet, decaying leaves in the fall. Hyperinflation, underinflation, black markets in currency – Venezuela, Poland, Argentina, Brazil, Taiwan trust and confidence is a problem for the individual notes themselves (is this one good?) and for all of them generally (will it stay stable?), spurred by the illegitimate producers, selling bricks of bills for pennies on the dollar to professionals in the business of laundering them through casinos, restaurants, laundromats and retail, and by the legitimate producers who may cause the value to climb too high or fall too fast and low.

Silver is silver; notes are notes. On what other basis could trust in money rest?

The Trust Bulb

'I'm done with Bitcoin', writes the anonymous contributor. 'It was easy money, but it wasn't worth the (literal) heat'.[28] This was posted in the summer of 2011, when Bitcoin mining was still a somewhat easy-money proposition. He or she spins a tale

[25] Javier Nieves, Igor Ruiz-Agundez, and Pablo G. Bringas, 'Recognizing Banknote Patterns for Protecting Economic Transactions', *2010 Workshops on Database and Expert Systems Applications,* 2010.

[26] Steven J. Murdoch, 'Software Detection of Currency', http://www.cl.cam.ac.uk/~sjm217/projects/currency/.

[27] Bernd Widdig, *Culture and Inflation in Weimar Germany,* Oakland: University of California Press, 2001.

[28] [Dubz mining], 'had 4 machines', 4chan.org, 2011-07-01 06:08.

of woe. They were running the mining machinery in their bedroom: four boxes of ‘overclocked 5850s,’ meaning graphics cards with chips optimized to execute certain classes of operations, whose performance had been pushed beyond the preset limit by adjusting the clock speed, the rate at which it performs those operations. They were using these chips to produce solutions to the challenges posed by the Bitcoin system by generating hashes of transaction data that meet the escalating difficulty set by the algorithm. Hashes are a very well established product in computer science, a way of producing data of fixed length from data of arbitrary length. And, like the P versus NP problems mentioned above, hashing problems (appropriately configured) can take time to solve but are very quick to verify when you want check if you’ve got a correct solution.

The Bitcoin system, from the original paper circulated by the pseudonymous ‘Satoshi Nakamoto’ up to the present state of refinement and implementation, takes advantage of this property in quite a brilliant way. Or, rather, it adopts a version of hashing from prior systems like Adam Back’s Hashcash proposal, which are in some ways more conceptually straightforward and easier to understand, so we’ll start there.[29] Hashcash was an idea for stopping the problem of spam email (among other uses). If it takes a little time to generate a unique hash of a message’s content, its recipient, and the timestamp of its sending, but almost no time to verify that the hash attached to an email is correct, then you can effectively ‘rate-limit’ the amount of email someone can send. When you send me a message, I won’t even notice that my email client has checked to confirm that the message you sent includes an accurate, unique hash particular to this message; nor will you notice that your machine has produced one – it only becomes an issue if you are sending, say, hundreds of thousands or millions of messages at once (as spammers must, to cast the net wide enough for a cost-effective catch of suckers and naïfs), in which case all those little hashes add up and render sending mass quantities of messages onerous. Your computers slow way down, the fans kick on, the heat billows from the vents.

Now imagine you have a network for transacting money that relies on all the nodes – everybody participating in the network – to verify that all the transactions taking place are accurate and above-board. To sustain confidence, you need to confirm that nobody’s making fake money and nobody’s spending the same money multiple times. Perhaps you can have all the nodes cast votes that each transaction accurately matches their record of what should be happening. What’s to stop many nodes under the control of one malevolent actor from casting masses of fake votes, and validating bad transactions? You rate-limit the process of validation. When participants in the Bitcoin system, or rather their machines, receive the updated ledger of transactions, they begin generating enormous numbers of hashes of the data, looking for one that meets a steadily escalating criterion of difficulty. Once it is found, they push their ‘answer’ out to the network, where it is swiftly confirmed by others; that block of transactions added to the blockchain, the master ledger, and they receive a batch of newly-minted bitcoins and all the transaction fees connected with that round of exchanges. To confirm a block of transactions yourself, fooling everyone else into

[29] Adam Back, ‘Hashcash – A Denial of Service Counter-Measure’, 2002, http://www.hashcash.org/papers/hashcash.pdf.

agreeing with you, it's therefore not just enough to have a bunch of fake voters under your control – you must be able to do more computational work than 51 percent of everyone else on the network, so you can consistently outguess them when it comes to generating hashes of the data.[30] There are other classes of attack on this system as well, most notably the 'selfish mining' protocol which uses a decision process in the ledger to manipulate what is taken as the definitive blockchain.[31] While these dangers are quite real, they don't undercut the interest of the idea: using limits within mathematics, computationally expressed, to establish a rigorous form of *timing* and build trust on that basis.

The bitcoins generated by 'mining' – that transaction validation process – are the only source of new bitcoins, meaning the ratcheting of difficulty is a throttle on the issue of new currency (making Bitcoin as a whole effectively deflationary, in ways that speak the cultic language of the Austrian school of economics). As users join the new network in the early days, adopters are rewarded by comparatively easy pay-outs from the system; as more sophisticated hardware and the associated powerful mining rigs and cartels hop on the bandwagon, the work entailed by mining goes up accordingly. It's very straightforward in practice: periodically, as the difficulty escalates, the system demands the hash of the data include an additional zero. This makes finding the correct hash proportionally more improbable – now it's not enough to find a hash valid for the data, but a valid hash like:

'00000000000000002b2d53213b1c58a82f728e2c80583f769436d6a2177c48d82'

which includes a whopping sixteen zeroes, all together, at the beginning. Stumbling across a number like this by guesswork is like hoping that a bunch of chimpanzees living in the jungle canopy will fix a crashed helicopter. To get these characters before others beat you to it on the network, and thereby get the new bitcoins and the fees, you need machines rated in terms of gigahashes per second – numbers of billions of possible hashes, produced every second. Which brings us back to the anonymous Bitcoin miner, in search of easy money, in their bedroom.

All that computational work doesn't come free, or even cheap. In the early days, it was possible to mine Bitcoin using your computer's CPU. Meeting the demands of the system soon escalated to GPUs – graphics cards, that is, better-engineered for cranking out hashes – and then, in short order, to ASICs. These Application Specific Integrated Circuits could be made to order for exactly one kind of work: not only to churn out hashes, but to meet Bitcoin's precise constraints. All this takes electricity, and all that electricity and consequent Joule heating means a new and awful world of dissipation to manage. The unfortunate miner with four mining rigs of 5850 Radeon graphics cards had been blessed with pretty good weather, so the room was 'warm, but tolerable' – but the fans on the enclosures were going at 100 percent already. The weather got hotter one day, and by the time he or she (luckily) woke up, they'd already

[30] Joshua A. Kroll, Ian C. Davey, and Edward W. Felten, 'The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries', *The Twelfth Workshop on the Economics of Information Security* (WEIS 2013), June 2013.

[31] Ittay Eyal and Emin Gün Sirer, 'Majority is not Enough: Bitcoin Mining is Vulnerable', arXiv:1311.0243v5 [cs.CR], November 2013.

developed heatstroke. Rushed to the ER, iced and hydrated, their story ended with permanent minor brain damage resulting from their brain swelling inside their skull, as though they'd barely survived a brutal malarial fever.

The photographs from the first round of Bitcoin's popularity, the images of people's awesomely eccentric home-built mining rigs, were pictures of improvised heat management. Box fans, big stretches of the corrugated tubing normally used to channel the waste heat from clothes driers, precariously poised air conditioners, and USB-powered fans resting directly on the finned heat sinks of boards were the rule. Stories abounded of early Bitcoin devotees rerouting their home flues to keep the warm, hash-generating air circulating through their houses in winter. The serious mining projects now, like Cloud Hashing in Reykjanesbaer, Iceland, and MegaBigPower in Washington (the state with the cheapest electrical rates in the U.S. due to an abundance of hydroelectric dams), are built on similar lines to the server farms described before: structured around efficient heat transfer through hot and cold corridors, with machinery neatly labeled in locked cages of perforated sheet metal, alight with flickering LEDs, and rows of Ethernet jacks.[32]

Iceland, Finland, Sweden, the Pacific Northwest: one detail has been left out of this overview of cryptocurrencies and heat, a detail easy enough to miss because it's too big to see. Every cooling system is really just a heat redistribution system, exporting heat from here (the apartment, the refrigerated truck cab or train car, the interior of the computer's chassis) to there. And 'there' is always ultimately the same there. The Earth's thermal system – atmosphere, hydrosphere, cryosphere, lithosphere, biosphere – is the terminal heat sink, taking both the dissipative heat, and the exhaust of whatever moves it from here to there. This is often carbon, the incineration of coal or gasoline for the power that keeps the fans on and the refrigerant pumping through the coils, and the electricity pushing through the chips generating all those gigahashes-per-second. The irony of this situation has escaped no one: a 'virtual' currency (requiring no bulldozer-dug bank vaults, idling armored cars, or 70-ton offset presses) which consumes a lot of electrical power in the form of cooling and computational work. 'Work', furthermore, that serves no purpose beyond limiting the issue of new coins and maintaining the trustworthiness of the blockchain – a system that is, as one says of an irksome person, difficult for the sake of being difficult. The ASIC machines custom-built for this purpose can't be used for anything else; if Bitcoin should wipe out as a currency they couldn't be retooled to simulate protein folding or composite special effects. There are entire Bitcoin spinoffs, altcoins, devoted to resolving precisely this sense of inutility, like Primecoin, which uses the proof-of-work process to find prime number chains of mathematical interest.[33]

'A lot': how much electricity does the whole Bitcoin system in fact consume? This keenly debated topic is full of untrustworthy, back-of-the-envelope estimates and calculations. The hyperbolic upper-bound estimates for Bitcoin's power consumption and carbon footprint (the whole nation of Cyprus! 0.03 percent of the world's total carbon

[32] Cloudhashing, https://cloudhashing.com/; MegaBigPower, https://megabigpower.com/.

[33] 'Sunny King' (pseudonym), 'Primecoin: Cryptocurrency with Prime Number Proof-of-Work', 7 July 2013, http://primecoin.io/bin/primecoin-paper.pdf.

output!)[34] are based on wildly varying numbers for the electricity demands made by different forms of mining equipment. Commentators look at the current gigahash rate, roughly average out the watts-per-gigahash demands of the mining equipment presumed to be most popular, squint, and end up with colossal numbers which can then be interpreted in terms of the megawatt hours in carbon according to some guesswork about countries in which mining takes place.[35] The lower-bound estimates, by contrast, tend to glide over the questions of infrastructure external to the work of pushing electrons around on ASIC boards – all that air conditioning. Many of the biggest mining operations enjoy significant economies of scale and make reference to various efficient load-balancing and energy management systems, all of which are of course proprietary. Hard numbers are hard come by.

Those we have, furthermore, are often framed by implicit moral arrangements in which Bitcoin work is 'waste', as opposed to really *useful* forms of computational work like running multiplayer online video games, streaming *Snow Dogs 2* and the abyssal ocean of pornography, and brokering and serving ads – to say nothing of energy costs for TVs and lights on in vacant rooms, half-empty refrigerators, inefficient homes, and the marquees in Times Square. In conversation with cryptocurrency advocates the question of the energy budget of conventional currency often comes up. Consider, they say, all those ATMs, guards with handguns, shipments from various mints and reserve banks, and the armored trucks loaded with hundreds of 500-dollar boxes of U.S. quarters, each weighing a bit more than 11 kilograms. To which we could add the ruined, alien-planet landscapes produced by the extraction of precious metals, the mountains of tailings and sumps of cyanide and mercury and other heavy metals. The gigahashes wasted in search of block authentication can look pretty lightweight compared to the deca-tons of waste ore produced and dumped to generate an ounce of gold.

Zoomed out to this scale – where we're weighing Bitcoin mining against the total cost of the circulation of currency, and following the transit of heat from the interior of the chip to the edge of the tropopause – we can see a useful similarity. 'Computational friction', writes Paul Edwards, 'expresses the resistance that must always be overcome, the sociotechnical struggle with numbers that always precedes reward.'[36] This strikingly apposite sentence is taken a little out of context, but fruitfully so. Edwards is writing, in *A Vast Machine,* about a different kind of heat management: the labor of recording, modeling, and understanding the global climate, and particularly the question of temperature, as the planetary heat sink's properties are changed by all the carbon (and methane, and various hydrofluorocarbons) added in. To understand this project as Edwards describes it we need to understand how hard it is to do things with data. Getting it into a useful format (a format that is itself a moving target as systems and platforms upgrade), checking and storing it, moving it to where it needs to be, employing it in operations, maintaining contextual knowledge about it: data friction, metadata friction, computational friction – think debugging, repairing, doing feature extraction, struggling at the Heisenbergian limits of modeling where complexity trades off against resolution.

[34] Guy Lane, 'Bitcoin's Carbon Footprint is out of Control', 19 December 2013, *bitcarbon*, http://www.bitcarbon.org/bitcarbon/.

[35] Michael Carney, 'Bitcoin Has a Dark Side: Its Carbon Footprint', *PandoDaily,* 16 December 2013.

[36] Paul Edwards, *A Vast Machine: Computer Models, Climate Data, and the Politics of Global Warming,* Cambridge, MA: MIT Press, 2010.

'It's not a bug, it's an undocumented feature!' It's an old programmer's joke: this weird unforeseen issue is actually (seen in the right light) functionality – the machine crashing whenever you try to edit *n*+1 documents at once is a helpful feature reminding you to go for a walk outside. This essay is about two big bugs, which cryptocurrency platforms refashion into complementary features. Computational friction, taking the most literal facet of Edwards' idea, turns the frustrating ceiling on computational work into a floor, a foundation, on which an institution (of sorts) can be built. The frustrating unreality of money, of the realness of any given note and trust in overall issue, is made explicit and featureful, with flawed open source code turning trust in all transactions that constitute the blockchain ledger into the basis of the trust in new money. (What makes the money money? The heat. What makes the heat valuable? That it's treated as the basis of the money.)

This is a system, in other words, in which the grain of the universe – the movement of particles, the collisions of electrons and ions – becomes a kind of friction brake on the operation of a social mechanism. Joule heating has been used as a source of visible light, and now it's been repurposed as a source of trust, a trust bulb. Like an incandescent bulb, it mostly produces heat, but it has trust as a side effect. Bitcoin's political baggage now runs the spectrum from those who'd like it 'boring', a regulated, taxed payment rail, to those who work to make it a source of great, fruitful chaos in the world, the infrastructure of an agorist society bringing down statist institutions. If we temporarily jettison that complex political cargo, it is revealed as an elegant, almost metaphysical parallel construction uniting computing and money.[37] Both are utterly quotidian matters that become mystical with a few pointed questions. What is it that gives money its value, built on nothing yet real enough to shape or deform the course of a life or a society? When does a physical system compute? Just about anything can be 'money' and move the agreements that constitute debt and credit. Given time, we can do the work of computing using pebbles in matchboxes, or water in ductwork, sticks and strings, cellular automata following rules.[38] The oblique ingenuity of cryptocurrency development was the realization that the awkward place where computing scrapes, friction-hot, against its physical substrate was precisely the place where a new kind of money could be built as an awkward fit between idea, confidence, trust, and material foundation. In their failure to be the perfect abstract models we understand them to be, lies the basis for a new, promising form where they meet in their deficiency. Made of nothing but hot air, technical ingenuity, and social fascination, the balloon takes off into the open sky.

[37] Tom Simonite, 'The Man Who Really Built Bitcoin', *MIT Technology Review,* 15 August 2014; Anti-statist: Oleg Andreev, 'Crypto-anarchy does not require anonymity', http://blog.oleganza.com/post/71410377996/crypto-anarchy-does-not-require-anonymity.

[38] See, for instance, the wonderful paper: Clare Horsman et al., 'When Does a Physical System Compute?', arXiv:1309.7979v2, 7 March 2014.

References

Andreev, Oleg. ‘Crypto-Anarchy Does Not Require Anonymity’, http://blog.oleganza.com/post/71410377996/crypto-anarchy-does-not-require-anonymity.

Back, Adam. ‘Hashcash – A Denial of Service Counter-Measure’, 2002, http://www.hashcash.org/papers/hashcash.pdf.

boyd, danah. ‘Blotchy Burns on My Legs from my Macbook’, *Zephoria*, 9 September 2007, http://www.zephoria.org/thoughts/archives/2007/09/09/blotchy_burns_o.html.

Cao, Xiaogang. ‘Visit of ASICMINER’s Immersion Cooling Mining Facility’, *Bitcoin Forum,* 25 November 2013, https://bitcointalk.org/index.php?topic=346134.0.

Carney, Michael. ‘Bitcoin Has a Dark Side: Its Carbon Footprint’, *PandoDaily,* 16 December 2013.

Cloudhashing. https://cloudhashing.com/.

Cray, Seymour. ‘U.S. Patent No. 4,590,538: Immersion Cooled High Density Electronic Assembly’, United States Patent Office, 18 November 1982.

Dayal, Geeta. ‘Max Mathews (1926-2011)’, *Frieze*, (May 2011), http://blog.frieze.com/max-mathews/.

[Dubz mining]. ‘had 4 machines’, 4chan.org, 2011-07-01 06:08.

Dyson, George. *Turing’s Cathedral: The Origins of the Digital Universe,* New York: Vintage, 2012.

Edwards, Paul. *A Vast Machine: Computer Models, Climate Data, and the Politics of Global Warming,* Cambridge, MA: MIT Press, 2010.

Eyal, Ittay and Emin Gün Sirer. ‘Majority is Not Enough: Bitcoin Mining is Vulnerable’, arXiv:1311.0243v5 [cs.CR], November 2013.

Fausset, Richard and Andrew Blankstein. ‘Films’ Fake Cash Can’t Look Too Real’, *Los Angeles Times,* 6 June 2001.

Godfrey, M.D. and D.F. Hendry. ‘The Computer as von Neumann Planned It’, *IEEE Annals in the History of Computing* 15.1 (1993): 11-21.

Hillis, William Daniel. *The Connection Machine,* PhD diss., Massachusetts Institute of Technology, Cambridge MA, 1985.

Horsman, Clare, et al. ‘When Does a Physical System Compute?’, arXiv:1309.7979v2, 7 March 2014.

Kant, Immanuel. *Dreams of Spirit-Seer by Immanuel Kant and Other Related Writings,* trans. John Manolesco, New York: Vantage Press, 1969.

King, Sunny (pseudonym). ‘Primecoin: Cryptocurrency with Prime Number Proof-of-Work’, 7 July 2013, http://primecoin.io/bin/primecoin-paper.pdf.

Kolodzey, James S. ‘CRAY-1 Computer Technology’, *IEEE Transactions on Components, Hybrids, and Manufacturing Technology* 4.2 (June 1981).

Kroll, Joshua A., Ian C. Davey, and Edward W. Felten. ‘The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries’, *The Twelfth Workshop on the Economics of Information Security* (WEIS 2013), June 2013.

Lane, Guy. ‘Bitcoin’s carbon footprint is out of control’, 19 December 2013, *bitcarbon*, http://bitcarbon.org/bitcarbon/.

Levy, Steven. *Hackers: Heroes of the Computer Revolution,* Sebastapol: O’Reilly Press, 2010.

MegaBigPower. https://megabigpower.com/.

Mihm, Stephen. ‘No Ordinary Counterfeit’, *New York Times Magazine,* 23 July 2006.

Murdoch, Steven J. ‘Software Detection of Currency’, http://www.cl.cam.ac.uk/~sjm217/projects/currency/.

Nieves, Javier, Igor Ruiz-Agundez, and Pablo G. Bringas. ‘Recognizing Banknote Patterns for Protecting Economic Transactions’, *2010 Workshops on Database and Expert Systems Applications,* 2010.

Reed, Fred. *Show Me the Money!: The Standard Catalog of Motion Picture, Television, Stage and Advertising Prop Money,* Jefferson, NC: McFarland, 2005.

Rosenbaum, Ron. ‘Secrets of the Little Blue Box’, *Esquire Magazine,* October 1971.

Schrader, Charles. *History of Operations Research in the United States Army, Vol. I: 1942-1962,* Washington D.C.: CMH Pub 70-102-1, 2006.

Simonite, Tom. ‘The Man Who Really Built Bitcoin’, *MIT Technology Review,* 15 August 2014.

Smail, Daniel Lord, Mary C. Stiner, and Timothy K. Earle. ‘Goods’, in *Deep History: The Architecture of Past and Present,* Oakland: University of California Press, 2012, pp. 219-240.

Sperry Rand Co. *UNIVAC I Maintenance Manual For Use With UNIVAC I Central Computer*, New York:

Sperry Rand Corporation, 1956.

Starosielski, Nicole. ‘Digital Media: Hot or Cool?’, *Flow* 15.5 (January 2012).

Unsigned obituary. ‘Charles Babbage, Philosopher’, *Van Nostrand’s Engineering Magazine,* October 1871.

Ware, Willis H., et al. *RAND and the Information Evolution: A History in Essays and Vignettes,* Santa Monica: RAND, 2008.

Widdig, Bernd. *Culture and Inflation in Weimar Germany,* Oakland: University of California Press, 2001.

Wolman, David. *The End of Money: Counterfeiters, Preachers, Techies, Dreamers – And the Coming Cashless Society*, New York: Da Capo, 2012.

Zhou, Rongliang et al. ‘Modeling and Control for Cooling Management of Data Centers with Hot Aisle Containment’, *Proceedings of the ASME 2011 International Mechanical Engineering Congress & Exposition*, November 2011.