Bitcoin and Cryonics

By Keegan Macintosh

In this article, I want to introduce you to Bitcoin, a topic that fascinates me *almost* as much as cryonics. Many *Cryonics* readers will have already heard of Bitcoin (certainly my first introductions to it were by members of the cryonics community), but in order to go on and talk about cryonics-specific uses for Bitcoin, I think it is important to give the actual technology a proper introduction, as well as a brief history of its creation and development. But perhaps most importantly, cryonicists have had important involvement in Bitcoin's inception and spread, and through the backward-looking lens of history, I believe this is a connection the cryonics community will be proud of. [At this point, I think it's important to make the following disclaimer: I own bitcoins, and am very optimistic about their future, both in value, and their potential as a highly positive disruption in the global financial system.]

What is Bitcoin?[1]

A "peer-to-peer electronic cash system" is what Bitcoin's creator, Satoshi Nakamoto called his idea in its initial design paper. The more wieldy name for Bitcoin and the many, lesser-known "altcoins" that have been developed in Bitcoin's wake, is cryptocurrency, the prefix *crypto* – referring to the fundamental role cryptography plays in its operation. Bitcoin is sometimes called a "virtual currency," and while this is certainly an easier way of communicating the general idea to the uninitiated, it does ignore what differentiates Bitcoin from other, equally "virtual" currencies in online games, such as World of Warcraft "gold" that has acquired real-world value (to the game's players, at least) and is traded for regular currency. Online merchants such as Amazon have also developed virtual currencies specific to their brands, as the next paradigm of prepaid gift cards and loyalty rewards programs. But all these other sorts of virtual currencies are ultimately controlled by a single entity – not unlike governments' control over their local currencies – whereas Bitcoin operates by consensus over a distributed peer-to-peer network. So bitcoins, World of Warcraft gold, and Amazon Coins are really apples, oranges, and bananas.

Others reject the "currency" characterization entirely, instead conceiving of Bitcoin as a "digital commodity." But to me, that simply begs the question of what features of the bitcoins themselves has commodified them? If it is their usefulness as a means of transferring value, are they not a currency first, and a commodity second? There is something of a chicken-and-egg aspect to that debate, so I will leave it to the economists and philosophers. Personally, I think it is more useful to define Bitcoin descriptively, in which case Bitcoin is a globally distributed ledger of transactions of a unit called "a bitcoin." A bitcoin has whatever value (in other currencies, or goods) that those who concur in Bitcoin's utility agree it has – voting with their traditional currencies by purchasing bitcoins with them. And so far, the global market's valuation of Bitcoin has increased by at least six orders of magnitude since it was released into the world in early 2009.

Now, the distributed ledger which forms the backbone of the Bitcoin network actually has a name of its own – the "blockchain" – so called because transactions between addresses of the network are recorded in the ledger in sequential "blocks" of data one megabyte in size. The transactions are collected into these blocks, verified for validity, and added to the blockchain by specialized users of the network, who must first "solve" the block by running it through a computationally intensive process called "hashing" until a particular result is reached, at which point that block is added to the chain and that user is rewarded with new bitcoins, along with any of the (optional) transaction fees included with the transactions in that block.[2] Because doing this work that keeps the network functioning is incentivized with the block reward, this whole process is referred to as "mining" bitcoins. The block reward halves approximately every four years, and the number of bitcoins will never exceed 21 million, though they can be subdivided further by adding additional decimal places as necessary.

Bitcoins reside at bitcoin addresses, which are rather unsexy strings of letters and numbers, like 14cD6PwopFAoeyPwtGAsSiMwJcLxS9ePC. However, these addresses can be represented as QR codes like the one to the left, which are a little more sender-friendly. Bitcoin is often referred to as an "anonymous" currency, but this really isn't true. Being a public ledger, it is only an anonymous system for a particular user if there is no way of tying their real-world identity to the transaction(s) that they wish to be anonymous. However, in contrast with IP addresses on the internet, one can have as many bitcoin addresses as one likes (and the private keys entitling them to transact with the bitcoins at those addresses), without ever paying for them or asking for someone's permission to have one. This is because the bitcoin addresses and associated private keys are all generated algorithmically, and the algorithm used to

define them provides for many more than enough for everyone on the planet (approximately 2×10^38 per capita, at present). Thus, *pseudo*nymity can be approximated by never using the same address twice, and this behavior is built into most Bitcoin wallet software by default.

A Very Abridged History of Bitcoin

Nakamoto's original design paper was posted to Perry E. Metzger's cryptography mailing list in late 2008.[3] The "genesis block" of the chain, containing the first 50 bitcoins, was brought into existence by Nakamoto in January of 2009, with the first version of the Bitcoin client released a week thereafter. Interest in Nakamoto's creation was sufficient to attract other developers to refine the protocol and the client, and design new clients – and of course mine for bitcoins, which at the time could be done with ordinary CPUs. In those very early days, it was not easy to pin any particular value on bitcoins themselves, but a now famous $25 pizza was ordered by one Bitcoin user at the request of another, in exchange for Ƀ10,000 in May of 2010. (At today's exchange rate, that pizza would now be worth nearly $1.3 million.) Two months later one bitcoin surpassed $0.01 in value, and later still in 2010, after the first major bitcoin exchange, Mt. Gox opened its virtual doors, $0.10. Bitcoin reached parity with the dollar in early 2011, hit $10 on June 2 of that year, and then "bubbled" up to over $30 within the next six days, before "popping" back to $10 and retreating all the way back down to $2 over the next six months. But by the second half of 2012, Bitcoin was back over $10, and jumped another order of magnitude to $100 during the first half of this year, shooting over $200 briefly in April before resettling to a (slightly) less volatile hover pattern around $100 over the months following. This more recent "bubble" received significantly more mainstream media attention, despite having a significantly more stable outcome than the 2011 bubble.

Personally, I prefer the characterization of these sudden upward price movements followed by downward corrections before resuming the long-term upward trend, as "hypermonetization" [4] events, as opposed to bubbles. Unlike tulips (the famous economic bubble example), Bitcoin has far clearer fundamentals supporting its increasing valuation by the global market. The more people that are exposed to the network and start using it, the bigger it gets, making it less vulnerable to attack, more useful as a currency, and more secure as a store of value (there is some debate around this, particularly around a possible trend towards *centralization* of mining on account of the more specialized and expensive equipment now required, but I think the general idea holds true). Furthermore, while the service-layer infrastructure around Bitcoin is still somewhat lacking – notably widespread, easy-to-use ways of turning traditional currencies into bitcoins and back again[5] – the existing financial transactions paradigm simply cannot compete with Bitcoin when it comes to transmitting wealth across the world as cheaply as to someone standing immediately next to you. Even PayPal has had to take note, and Western Union, too.[6] In addition to becoming an accepted form of payment with more and more online merchants (and even some brick-and-mortar ones) every day, bitcoin mining has become an industry in its own right, due to the ever increasing difficulty of the mining algorithm. Difficulty increases are a design feature of the protocol intended to secure it from a malicious entity simply amassing enough computing power to centralize control over the network, thereby destroying its primary fundamental value. Thus, the required hardware for anyone looking to derive profit from mining has graduated from regular old CPUs, to high-end GPUs, and now finally to chips specifically designed for the task (application-specific integrated circuits, or ASICs). Setting up and maintaining GPU "farms," and now, more recently, developing and deploying ASICs has required significant investment, precipitating the arrival of "virtual" companies that raise capital through Bitcoin IPOs on virtual securities exchanges, sharing the profits back with the "virtual" shareholders. (This of course being a securities regulator's nightmare, but we'll leave that alone for now.)

Early Connections to Cryonics

By now, you are probably wondering how any of this relates to cryonics. Perhaps it would surprise you to know that one of Alcor's long-time board members' names is written right into the Bitcoin protocol? Indeed, without Ralph Merkle's work in cryptography some decades prior, Bitcoin might not even exist – or at least not in its current form. Public key cryoptography, for which Merkle was inducted into the 2011 National Inventors Hall of Fame, is a core enabling technology of Bitcoin. A cryptographic data structure called a "Merkle tree" (and associated "Merkle root") is an integral part of the bitcoin hashing algorithm, so our illustrious Mr. Merkle's work is essentially stamped on every block in the blockchain. While Merkle's website does not indicate a personal interest in bitcoins, it does include the following foreboding prediction:

> *"The likely development of quantum computers (QCs) in the next one or two decades would compromise all widely used public key cryptosystems (PKCSs)… [I] t may already be too late to deploy a QC-resistant PKCS standard throughout the world before quantum computers become available. […] The developers of a quantum computer are likely to keep its existence secret for some time, during which time they could freely forge signatures for any system that was not QC-resistant: signatures that most would find hard to dispute."*

That being said, the Bitcoin community is aware of the threat quantum computing could represent (a threat to which the traditional financial transactions institutions, i.e. banks, credit card networks, etc., will be highly vulnerable as well), and already has ideas of how to upgrade the protocol's security when necessary.[7] Regardless, Ralph Merkle's contributions to cryptography have made possible a major leap forward in the very idea of what money can be.

But the early connection between Bitcoin and cryonics goes further. A man named Hal Finney was an early responder to Nakamoto's initial posts to the cryptography mailing list, and ended up being the recipient of the very first bitcoin transaction, from Nakamoto himself in early 2009. Finney also identified a specific kind of double-spend attack possible against merchants who accepted payments without waiting for network confirmations of the transaction, which has been given the name the "Finney attack." Finney was also a member of the Less Wrong online community (created by well-known cryonicist and Friendly AI researcher, Eliezer Yudkowsky), and later in 2009, Finney posted to Less Wrong that he had been diagnosed with ALS.[8] In the responses to Finney's post, Yudkowsky asked him if he had cryonics arrangements in place, to which Finney replied that he had been an Alcor member for 20 years. Finney's involvement on Bitcoin forums and Less Wrong did diminish over time, but after the 2013 price rise, Finney made a post on bitcointalk.org relating his early involvement in Bitcoin's development, his diagnosis with ALS, and his continued work developing more secure Bitcoin wallet clients.[9]

The Mystery of Satoshi Nakamoto

An interesting twist in the story of Bitcoin is that the true identity of its creator is not known. Satoshi Nakamoto's writing style, and the timing of his daily activity/inactivity cycles have led many to doubt that he was the 37-year old Japanese man he claimed to be, with some even suspecting that Nakamoto was a singular virtual identity masking a group effort. Having written the first Bitcoin client himself, Nakamoto's coding has been described as "elegant in some ways and inelegant in others," potentially indicating that Nakamoto was not a professional programmer, though not a complete amateur either.[10] Whoever he/she/they was or were, Nakamoto's involvement in the project waned over the course of 2010, and the task of continuing to refine Bitcoin has become a collaborative effort clustered around one person who is paid to develop the protocol full-time.[11]

But in honour of Satoshi Nakamoto's grand idea, the (current) smallest subunit of a bitcoin, Ƀ0.00000001, is called a *satoshi*. And boy-oh-boy, does Satoshi ever have a lot of satoshis! As one of the earliest dedicated users and miners, at a time when mining could be done with ordinary CPUs and the network was not nearly as distributed as today, Nakamoto amassed quite a hoard of bitcoins. However, since his disappearance in 2010, the lion's share of the bitcoins traced back to the protocol's creator (over a million of them) were never spent.[12] Depending on the real-world identity of the person or persons behind "Satoshi Nakamoto," and the underlying motives behind creating Bitcoin and then retreating away right as it started attracting real attention to itself, maybe those coins will never be spent.

Legal Status of Bitcoins

Part of the reason Bitcoin is difficult for lawmakers and regulators to categorize is because it does not lend itself to analogy very well. Or perhaps it does this *too* well – that is to say Bitcoin can be meaningfully analogized to different and competing schemas. Fundamentally, as I discussed in the first part, Bitcoin is a ledger of transactions. But normally, a ledger of transactions refers to a unit which represents some *physical thing*, and even if that physical thing rarely actually changes hands in the vast majority of transactions of it, somewhere there is some form of *property*, in the legal sense, that the ledger is tracking. Even where this property is just a "right" to something else (think shares in a company), there's usually some material thing (often money) at the end of the line.

Even bank notes and coins, the physical manifestations of traditional currency, are "referring" to something else – namely the respective territorial government's acceptance of that currency for payment of taxes, etc., and its authority to insist that merchants within the territory accept the currency as "legal tender." Sometimes the governments will have some kind of reserve of another valuable thing (like gold) in place to "back" the value of its currency, but in more recent times this has become less common, and a territory's currency has value by government fiat. Bitcoin defies all this. There is nothing "backing" Bitcoin, only communal trust in the protocol itself, which is basically faith in cryptography and in the Bitcoin community's collective will to see the project succeed. And so, Bitcoin defies or at least confuses the current legal conceptualization of what property *is*. Could it be said that a Bitcoin user has "rights" to particular bitcoins, even though they don't actually exist anywhere other than on a ledger? Or does it make more sense to say they have exclusive rights to the address and private key that they have claimed for themselves – even though those were generated by a publicly available algorithm, with some real (but very, very, *very* small) chance that someone else could randomly generate the exact same ones, and be able to transact any bitcoins happening to be there..?

Other virtual currencies, like World of Warcraft "gold" and Amazon coins, while conceptualized as currency, derive their value, and any legal rights their users may have, from the contract agreed upon between issuer and user (however cursory that agreement may have been). Often, these agreements actually bar the user from trading the virtual currency to another user in exchange for traditional currency, and the issuer reserves the right to unilaterally change the contract on notice to the user. Nevertheless, the users of these currencies do have some legal rights, arising out of contract.

Bitcoin defies this too. There is no single issuer, and no one entity has the ability to change the Bitcoin protocol. The limit of the "powers" of those most closely involved with developing the protocol, is to release an update to the basic client, which

is open source, and suggest that the update be adopted by the many users of the network – miners in particular. For major changes, all users must accept the update or risk a "hard fork" of the blockchain, with two parallel ledgers each purporting to be a true representation of the state of the network. Thus, it needs to already be a foregone conclusion that a large majority of the network will accept such major changes before it is even released, else doing so will undermine the project itself. In legal terms, we could perhaps conceive of the Bitcoin protocol as a multi-party, majority-guided, consensus-driven contract regarding the formulation of a ledger of transmissions of a unit that all the contractors accept have some value – value derived from the nature of the system thus described. But this "contract" is written in computer code, and is constantly self-executing (or to continue the metaphor, self-enforcing) in real time all the world over. And far from a simple contract of sale or services, or even a complex corporate transaction, the Bitcoin contract describes an entire economic system, not tied in any way to the geographic territories its users reside in, or, more importantly, the laws of those territories. Bitcoin is living law, created, sustained and refined by the supranational community of its users.

Now, with all that said, it is still completely within the purview of courts and lawmakers to "admit" bitcoins as a form of property. And while it is still early days, it appears that at least one court has done just that. In an early ruling in the prosecution of a rather notorious Ponzi scheme involving Bitcoins, a Texas District Court judge ruled that "Bitcoin is a currency or form of money," and thus the defendant's claim that Bitcoin was not money and therefore his offerings were not securities within the jurisdiction of the SEC was baseless.[13] Also, the Financial Crimes Enforcement Network ("FinCEN"), the anti-money laundering enforcement agency of the U.S. Treasury has stated that both bitcoin exchanges as well as miners that exchange their newly-mined bitcoins for money are money transmitters subject to state licensing requirements – though how and why this would be enforced against the latter group is unclear to say the least.[14]

Meanwhile, up north, the Canada Revenue Agency has indicated that the rules which apply to bartering apply to trades involving bitcoin, which means that purchases of goods, services, or other currencies with bitcoins will result in taxable capital gains (or losses) if the value of the bitcoins (in Canadian dollars) has increased or decreased since they were acquired.[15] And, in contrast with the U.S., Canada's Financial Transactions and Reports Analysis Centre ("FINTRAC"; agency equivalent to FinCEN) has informed bitcoin exchanges that they are not subject to regulation as money services businesses under the applicable anti-money laundering laws (for the time being, at least).[16]

Other concerns regarding the technology

Aside from uncertain, sometimes conflicting legal classification and treatment, other concerns have been raised regarding the use of bitcoins in illegal drug and weapons trade, and for money laundering by criminals and terrorists. However, these arguments flounder somewhat when faced with the simple fact that as a *public* ledger, it is technically *easier* to trace dirty bitcoins than it is to trace dirty cash. That said, bitcoin mixing (read: laundering) services have sprung up for bitcoins too. It is worth noting here that the Silk Road, one of the largest marketplaces for all things illegal, operating on the near-anonymous Tor network and using bitcoin as its primary trade currency, was recently shut down by the U.S. government – its alleged operator arrested on drug charges and conspiracy to murder.[17]

Others point to the fact that it is possible to use the Bitcoin protocol to encode other kinds of content into the blockchain – including illegal content, like links to child pornography – immortalizing it there in the computers of every user of the network (whether they have the means or the desire to decode the content or not). Of course, this is not a new argument – it has been leveled against the Internet itself. And like the Internet, the Bitcoin protocol cannot be held responsible for the moral acts of its users, good or bad. Law enforcement agencies will simply adapt, as they already are doing.

The above is by no means an exhaustive analysis of the legal status of Bitcoin or of any particular uses for the technology, it is just meant to give you an idea. Generally speaking, owning and using bitcoins seems to be legal, but doing things with Bitcoin that would be illegal to do with money or with the Internet, remain illegal. It's as simple as that.

Cryonics-specific uses for bitcoins

(1) Asset preservation

It has been suggested that since bitcoins appear to store value (in a somewhat erratic, volatile fashion, if that isn't a contradiction in terms), they could provide an alternate means to those currently employed by cryonicists seeking to maintain possession of their accumulated wealth during their period of cryopreservation (namely, asset preservation trusts). And in fact, since Bitcoin is designed to be a deflationary currency[18], assuming that it survives and is adopted widely, wealth stored as bitcoins will likely be worth much more in the future than it is now. This might be attractive to cryonicists for whom volatility on shorter timescales is not terribly concerning.

So how could cryonicists accomplish this? The all-important piece of information that gives a particular person the ability to send bitcoins stored at a particular address is the private key for that address. Trouble is, no matter how that private key is stored, whether digitally on a computer owned by the cryonicist, or on a secure cloud server controlled by the cryonicist under some agreement entered into with the cloud server provider, or even written down on a simple piece of paper (the so-called "paper wallet"), none of these records of the private key will escape

the effects of estate law if they remain the cryonicist's property upon legal death. Thus the information required to transmit the cryonicist's bitcoins would end up in the hands of beneficiaries – beneficiaries who today might not even know what to do with them! This could result in either the loss of the bitcoins to the cryonicist, or the permanent loss of the bitcoins altogether, since if the private key is outright lost, the bitcoins stored at that address are no longer accessible.

The only way to avoid this would be to use essentially the same mechanism currently used for cryonics asset preservation, i.e. giving the medium with the private key on it to a trustee to hold for the cryonicist until they are successfully resuscitated. But then we haven't actually come up with a new solution to the problem we set out to solve, because this trust will have to be drafted in more or less the same way as other cryonics asset preservation trusts, such as the Alcor Model Trust, with an interim beneficiary standing in for the cryonicist while they are not a legal person. And there is nothing wrong with that in principle, but since bitcoins are informational in nature, there might be another way of preserving them for later use, without using trust law mechanics – perhaps as a way of hedging oneself against the possible failure of the trust for one reason or another.

This alternate method relies on the fact that, as information, bitcoin private keys can be *memorized*. However, private keys are even longer than bitcoin addresses themselves, and thus not the easiest things to memorize. So, some clever people have devised a way of generating private keys by hashing, using series of words that are much easier for the average human being to remember, like "correct horse battery staple."[19] These approaches to securing bitcoins are referred to as *brain wallets*. Fair warning, though: short, simple combinations of ordinary words are vulnerable to "dictionary attacks." For similar reasons, a beloved section of poetry, in unaltered form, is not a wise choice of phrase to generate a private key either. As with ordinary passwords, addition of numbers, special characters, and variations of case are advisable.

In their brain wallet, the cryonicist stores some of their wealth in bitcoins using a secret passphrase known only to them. Upon resuscitation, they generate the private key from the passphrase, and they have everything they need to transact with the bitcoins as they desire. Conceivably, brain wallets could even be used to incentivize resuscitation, by telling your cryonics provider about the bitcoins and promising them some portion of them upon your return.[20] Of course, that idea leads to a potential pitfall of storing the key to your wealth in your brain, as it makes your brain potentially quite valuable – that is, valuable to people other than yourself and those that care about you for *you*. If it became common knowledge that cryonicists were using this as a strategy for asset preservation, mightn't this make cryonics facilities attractive to the future's version of tomb-raiders, lusting after the riches locked away in cryopreserved brains? The best case scenario would be that the technology exists to somehow "read" the private key from a brain while still cryopreserved. A worse scenario would be that the cryonicist, having been abducted from their long-term care provider, is later resuscitated under rather different circumstances than they intended – as hostages of their resuscitators, and only of continued value to them until they give up the goods, as it were. I will say however that both those scenarios sound more like premises for science fiction stories than likely futures.

Another, less fantastical problem with using brain wallets for asset preservation is the possibility that part of the cryonicist's brain that is involved in storing the private key – or more likely the passphrase used to generate it – is damaged during cryopreservation in a way that is not reparable. However, without delving too far into the subject, I wonder if there are mnemonic strategies that would reduce the likelihood of this undesirable outcome. Even something as simple as ritualized, periodic recall of the passphrase to continually reactivate the memory and strengthen it might result in a memory that has sufficient physical redundancy in the brain to resist some amount of damage.

Lastly, there is always the chance that during the patient's cryopreservation, Bitcoin fails for some reason, either because some major flaw in the protocol is discovered and exploited, or a successor technology comes along, and the value and wealth currently stored in Bitcoin drains out of it into the successor. That said, Bitcoin still has a strong first mover advantage, and as a protocol, any deficiencies identified through experimentation with the numerous "altcoins" that exist can simply be implemented into Bitcoin, which has considerable network effect favouring its competitive survival. However, due to this and the aforementioned risks, it would be seriously inadvisable to make storing wealth in Bitcoin brain wallets one's *only* asset preservation strategy.

(2) Collection of donations, and payments for services

Case in point: I created a Bitcoin address for the Institute for Evidence Based Cryonics just before the symposium on Resuscitation of Cryonics Patients in May, and merely because we accepted bitcoins, someone in the audience, with whom we had no prior relationship, made a donation. And all he had to do was scan the QR code of IEBC's public address that was on my phone.

In addition to soliciting donations this way, cryonics service providers could also accept member dues and lump-sum prepayments via Bitcoin. Compared with the transaction fees charged by credit card companies and PayPal, which are generally a percentage of the value of the transaction itself, the default suggested transaction fee is only 0.0001, or at today's exchange rate a little over one cent[21]. And historically, as the

price of bitcoins has increased, the default transaction fee has been reduced, since transaction fees only need to be a small component of the miners' incentive while the block reward is still quite high. Anyway, this is much cheaper than the competition, and also much faster, as Bitcoin transactions "settle" securely in about an hour, and realistically can be relied on even sooner when dealing with relatively small transactions, as the risk of a doublespend attempt is very low there due to the cost of the computing power required to successfully pull it off.

However, for organizations worried about the extra level of accounting complexity created by accepting payments in a currency with a value that fluctuates relative to their home currency, there is an alternative. Numerous payment companies are springing up in the Bitcoin service layer that aim to make accepting bitcoins easier on companies, Coinbase being a wellfunded frontrunner that gives merchants the option to have incoming bitcoin transactions converted immediately into USD at the current exchange rate, plus a 1% service fee (which is still significantly cheaper than credit cards and PayPal).[22]

Other cryonics-relevant uses

The surface has only just been scratched with respect to what the Bitcoin protocol is capable of. Blockchain technology is an incredibly powerful tool, that has already been adapted for use as a cryptographically secure, peer-to-peer messaging system[23], as well as a decentralized domain name system[24]. Automated contracts with built-in dispute resolution mechanisms, aka "smart contracts" are in the works, and "smart wills" should be possible as well, though cryonicists will probably be more interested in ways of maintaining personal control over their wealth, as described above.

Conclusion

Hopefully, this article has served as an understandable yet accurate introduction to Bitcoin, from both a technical and a legal perspective, with special attention to its historical connections to the cryonics community, and its possible future uses for cryonics. ■

Learn more: http://bitcoin.org/en/

Previously published as a two-part article in *Cryonics* magazine October and November, 2013

ENDNOTES

1 For those who might be irritated by my switching back and forth between "Bitcoin" and "bitcoin," the capitalized former is usually reserved for referring to the protocol as a whole, whereas the non-capitalized latter refers to units of the currency itself.

2 Transaction fees are not required to broadcast a transaction to the network, but miners can opt only to include transactions with fees in any blocks they solve, so including a fee will result in faster confirmation by the network. The current default fee (no matter how large the transaction) is Ƀ0.0001 – approximately one cent.

3 http://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html

4 http://konradsgraf.com/blog1/2013/4/6/hyper-monetization-questioning-the-bitcoin-bubble-bubble.html

5 That said, the world's first operational Bitcoin ATM will be installed in Vancouver this month, with four others in Toronto, Montreal, Calgary and Ottawa: http://www.ibtimes.com/worlds-first-bitcoin-atm-coming-canada-robocoin-kiosk-hits-vancouveroctober-1404346

6 http://blogs.wsj.com/digits/2013/04/30/could-paypal-be-on-horizon-for-bitcoin/

7 http://bitcoinmagazine.com/6021/bitcoin-is-not-quantum-safe-and-how-we-can-fix/

8 http://lesswrong.com/lw/1ab/dying_outside/

9 https://bitcointalk.org/index.php?topic=155054.0

10 https://en.bitcoin.it/wiki/Satoshi_Nakamoto

11 Gavin is paid a salary by the Bitcoin Foundation, a non-profit working to standardize, protect, and promote the Bitcoin protocol: https://bitcoinfoundation.org/

12 https://bitslog.wordpress.com/2013/04/17/the-well-deserved-fortune-of-satoshi-nakamoto/

13 Securities and Exchange Commission v. Shavers, No. 4: 13- CV-416 (E.D. Tex. Aug. 6, 2013).

14 "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," FIN-2013-G001. Available at http://fincen.gov/statutes_ regs/guidance/html/FIN-2013-G001.html

15 http://www.cbc.ca/news/business/revenue-canada-saysbitcoins-aren-t-tax-exempt-1.1395075

16 http://www.theregister.co.uk/2013/05/20/canada_ welcomes_bitcoin_traders_fintrac_letter/

17 http://www.reuters.com/article/2013/10/02/us-crimesilkroad-raid-idUSBRE9910TR20131002

18 The mining reward will halve approximately every 4 years, resulting in the total number of bitcoins never exceeding 21 million – the design rationale being that over time the number of transactions on the network will increase to the point where competition for rapid inclusion in blocks (and thus, faster confirmation of the transactions) will result in sufficient transaction fees to incentivize miners' continued support of the network without the block reward. So while technically the supply of bitcoins is increasing, it is expected to eventually behave like a deflationary currency, relative to traditional currencies. Since 25 new bitcoins are created approximately every 10 minutes, at present over $3,000 USD worth of "new money" in traditional currencies needs to enter the bitcoin market just for the price of bitcoins to remain flat; thus, the rising price of Bitcoin, while appearing like deflation, is actually merely a function of supply versus demand (and also exchange bottlenecks).

19 This example is rather famous in the Bitcoin community, as it was used in the popular online comic strip, xkcd: http:// xkcd.com/936/

20 I must credit this idea to Danila Medvedev, who floated it on Cryonet Asset Preservation mailing list in August: http://groups.yahoo.com/neo/groups/New_Cryonet/ conversations/messages/5448 (requires joining the mailing list to view).

21 Remembering that the transaction fee is only required if you want your transaction confirmed relatively quickly. If there is no rush on the recipient's end, one can send bitcoins without any fee at all, though it may take some time to be included in blocks, as transaction fees are part of the miners' incentive, though for now a relatively small incentive compared with the 25 bitcoin block reward… but this will change over time.

22 https://coinbase.com/merchants

23 https://bitmessage.org/

24 http://dot-bit.org