"Epsilon Theory Mailbag: Bitcoin and Big Data"

One of the best parts of authoring Epsilon Theory is the correspondence I get from readers. For the past few months, however, I've been frustrated by my inability to respond to every writer with the same attention and thoughtfulness evidenced by their emails. Between my day job and the effort each Epsilon Theory note requires, I've run out of hours in the day to respond to the geometrically increasing volume of emails I receive. Having a public comments page on the website isn't a solution for a number of reasons – some of my correspondents don't want to be public, I still wouldn't have time to respond to the comments, an anonymous comments page tends to become a cesspool, and the regulatory burden this would place on Salient is not insignificant – so I've decided to start an irregular mailbag column. For the most part I'll be aggregating common comments and questions with a few recent news articles, and I won't reprint anyone's private email communication without asking permission first. Along the way I'll try to work in some of the more insulting comments published on the public/anonymous comments pages of *ZeroHedge*, *Seeking Alpha*, and *Forbes Online*, as well as some lovely Tweets … it's important to keep a sense of humor about this stuff!

For this initial effort I'll focus on reader comments to "The Effete Rebellion of Bitcoin" and "First Known When Lost", two recent notes that sparked more than their fair share of responses.

You, sir, are using glib, provocative, and insulting descriptions to pull in readers, then doing a bait & switch.
-- Elizabeth VH

Well … yeah.

If bitcoin is just a fad, what do you consider the Internet?
-- @PerianneDC

Not very smart. Surprised Forbes published him. Spouting bs before enlightenment is a common trait of effete snobs.
-- @jmwnuk

These were fairly typical comments from the Twitterverse. As someone who has been called the a-word, the b-word, the c-word (yes, the c-word), the d-word, the f-word, and the s-word on the mean

streets of *ZeroHedge*, I find Twitter haters to be almost charming in their child-like Peewee Herman-ish insults. For the record, I suspect the Interwebs are here to stay. And, dude … I know you are, but what am I?

You're an idiot. Ever heard of 2-factor authentication?
-- many anonymous comments, surprisingly few emails

I love 2-factor authentication. I love anything that allows me to keep the same password for more than a few months and avoid the "security theatre" that so many enterprises portray by requiring me to change a password for absolutely no reason other than that it looks like they're actively defending my security.

Banks love 2-factor authentication, too. Why? Because it provides a significant security upgrade for the online account transfers that federally regulated banks are *required* to offer per the Electronic Fund Transfer Act of 1978. Yes, 1978. The same year that TCP/IP was invented. Jimmy Carter vintage legislation for an Internet that wasn't even a twinkle in Al Gore's eye and a retail banking world where ATM's were novelties. Banks aren't rolling out 2-factor authentication protocols in 2015 because it's a convenience for *you*. They're rolling it out because it's good for *them*, because it helps limit (but by no means eliminate) the losses they suffer from the online transaction liabilities imposed by Reg E of the 1978 Act. It's exactly like a credit card issuer shutting down your card when you go on vacation. In no way is this "for your protection"; it's all about limiting their liability for charges made on a stolen card. And even with the enhanced security of 2-factor authentication, notice how the transaction size of all online transfers is limited to an amount that the federally mandated blanket bond will cover. Take away that federally mandated insurance backstop and federally mandated online transaction liability and you've got Bitcoin – a Hobbesian environment where security and risk management is *entirely* on you, and where in a very real way life is "a war of all against all". Yes, it's invigorating and refreshing to be occasionally free of Leviathan and its mandates on this and mandates on that. But only in small doses, thank you very much. Sorry, but I've read Thomas Hobbes and seen "Jeremiah Johnson" too many times to be more than a tourist when it comes to modern crypto-anarchy.

Speaking of Leviathan … one-time 2-factor authentication requires a delivery device or token, and on a mass scale that means text messages over smart phones. Does anyone in his or her right mind believe that a cryptography system that generates a second key and texts it to you on your registered

cellphone is unhackable or untraceable by any number of national security services? Really? Read this if you do.

You're an idiot. Ever heard of multiple private key systems?
-- many anonymous comments, surprisingly few emails

I love multiple private key systems. I appreciate them in the same way that I appreciate an intricate clock. I appreciate them in the same way that I appreciate the medieval voting system to elect a Venetian Doge. Wait … what? For more than 500 years, from 1268 – 1797, the Supreme Leader of The Most Serene Republic of Venice was elected for a life-time term by means of a highly complex ten-step process, where groups of electors were alternately randomly selected by lot and then directly selected by the votes of those selected by lot, over and over again for 5 of these dual rounds. The process was designed to prevent any single faction from corrupting the election through bribery or by "packing the court", and … it worked. Venice maintained a stable oligarchy for hundreds of years, an unbelievably difficult feat in any age (for a fascinating analysis of the Doge electoral system and its implications for security protocols, see this paper by two HP scientists).

But it worked at a cost. Direct costs, opportunity costs, complexity costs … you name it, stability and elegance do not come cheap. There is an unavoidable and linear (or worse) relationship between security and cost. Or rather, the cost of breaking the security of a system does not increase faster than the cost of advancing the security of that system, whether you're talking about multiple keys or longer passwords or extra voting/lottery election rounds. There is no such thing as a free lunch, particularly when it comes to information entropy, which is what we're really talking about here.

The problem is that the cost of complexity in Bitcoin's case is only manageable in a commercial sense if you inject third party service providers into the mix. Now there's a long history of successfully injecting such third parties into financial transactions. In fact, no large property or securities cash transaction occurs today without a government-regulated escrow agent playing the central role of validating the underlying transaction. If I buy a house or 100 shares of Apple, my money isn't released to the seller until a government-certified and insured intermediary makes sure that I have clear possession of that property or block of securities. Why is this a good thing? Because if something goes wrong with the underlying transaction … if all is not as advertised with the property or securities I am purchasing … I have recourse. Ultimately, I have a government and a government's self-interest and a government's guns on my side. None of this exists in the Bitcoin ecosystem, and any entity that holds

itself out as an escrow agent or transaction validator does so without a smidgen of government support beyond what's available to the local laundromat. Would I take a non-regulated escrow agent at their word if I'm buying a skim latte or a snappy new suit of clothes? Sure, why not. No biggie if the deal falls through, and at least I'll have an interesting story to tell. Would I take a non-regulated escrow agent at their word if I'm buying a house? No way.

I know that no one in Bitcoin-world likes to think about Mt. Gox, and I know it was a flawed animal … a complete outlier from all of the brilliantly conceptualized and elegantly implemented Bitcoin and blockchain service providers that got their VC money and set up shop over the past 18 months. I'm not arguing otherwise. My point is simply this: once a Bitcoin service provider gets big enough … once there are a couple of hundred million dollars sloshing through your system … you're going to be robbed. I don't care how smart you are or how much you trust your employees and your systems, you're going to be robbed. Now maybe you can find private insurance against the small stuff. But public insurance – which is the only thing that works in a big crack-up and has been part and parcel of the mainstream banking world for 80 years – is not available to you. There's not a government in the world that really cares whether a Bitcoin service provider in its jurisdiction lives or dies, and that's a problem. I want my bank and, by extension, my bank account backstopped by infinite lawyers, guns, and money (to quote the late, great Warren Zevon). And that's what modern governments provide – infinite lawyers, guns, and money. The Venetian electoral system worked for 500 years not only because it was elegant and smart, but also because Venice had the largest navy and the biggest Treasury in the Western world over that span. That's systemic security, and that's what I want underpinning my elegant and smart financial service applications.

Bitcoin might have its flaws, but banks worldwide already allow direct trade - directly from bank account to bank account: http://cointelegraph.com/news/113537/german-bank-unveils-insured-express-bitcoin-buying-moves-into-us-market
-- Monic DG

Am I surprised that an online-only German micro-bank (200m euros in deposits as of 12/31/13) is trying to gain publicity by claiming that Bitcoin transactions and deposits are now linked to insured accounts in euros or dollars? Of course not. But even here dig just one inch below the surface claims and you see that Fidor Bank is linking Bitcoins to an ordinary cash account in the same way that Bank of America might link your insured cash account with a personal check you want to deposit or a registered security you want to sell. I mean … if you give a bank 3+ days for the transaction to clear, you can get pretty much anything deposited to a cash account, but that's a far cry from saying that

depositing a personal check is the same thing as depositing cash, particularly if the personal check is for anything more than a trivial amount.

You mention Silk Road in passing. Have you read the *Wired* transcripts of the Dread Pirate Roberts trial?
-- Bill E.

Wow. Everyone who doubts that Bitcoin is inextricably entwined with illegal activity, and not always of the victimless sort, should read the transcripts of the phone conversations between Silk Road founder Ross Ulbricht (aka Dread Pirate Roberts) and a senior manager for a regional Hell's Angels franchise (aka Redandwhite), presented at Ulbricht's federal trial. My conclusions:

1) If there aren't 20 screenplays making the rounds in Hollywood based on this transcript, I will eat the accumulated print outs of every Epsilon Theory note to date.
2) Every company is a technology company today. Even the Hell's Angels.
3) Redandwhite would be a successful businessman in any century and any profession.
4) As always, life imitates art. Hyman Roth: "I'm going in to take a nap. When I wake, if the money's on the table, I'll know I have a partner. If it isn't, I'll know I don't." Redandwhite: "I will check the computer in about 10 hours, and if I see that you want to go ahead with this and the payment has been sent, we'll do it today." [hat-tip to Todd C.]
5) The murders-for-hire here are made possible by Bitcoin. Period. You think Ulbricht would be wiring cash or taking suitcases full of small bills to Vancouver? Please.

Bitcoin (or, if Bitcoin fails, some replacement cryptocurrency) represents a reversal in the rule/permission cycle, applied to ownership, in a similar way that the Internet as a whole represented a reversal in the rule/permission cycle applied to communication.

What I mean is: Neither the Internet (or any application of it, like email) fundamentally challenges the existence of certain legal rules. It *does* however fundamentally change the order in which you can proceed to do certain things: before the Internet, you needed to ask for permission more often than not (for example, to publish something), at which point a "rule check" took place.

The Internet reversed this process: the rules still exist, and you can still be prosecuted for breaking them, but the *first* step is your decision if you want to do something that could potentially break those rules or not: you can post whatever you want, on a number of places. Whether it's legal or not is a different thing, but that check occurs *after the fact* of you posting it.

This is where Bitcoin comes in. A distributed, tamper-proof (by our best knowledge on the matter) way to register and transfer ownership rights nearly instantaneously, over arbitrary distances *without* the need to ask any authority for permission to do so, is a major step.

-- Wouter D.

This is a *very* smart observation. Wish I had thought of it. The Internet is indeed a Great Leveler, a force for disintermediation that rivals the printing press, and no social practice – including the social practice of Money – is immune to that force. Thanks, Wouter.

Moving on to Big Data …

Big data is like teenage sex: everyone talks about it, nobody really knows how to do it, everyone thinks everyone else is doing it, so everyone claims they are doing it.
-- Speedy W.

Me and my team at work use big data all the time and I can tell you first hand it's almost useless. SaaS and Cloud Computing were wearing thin so big data was needed to continue Silicon Valley's only real talent: separating fools from their money.
-- "TS"

There's no doubt that "Big Data" has become a marketing catchphrase, much like "The Cloud". But my guess is that TS "and his team" are using Big Data in approximately the same way that free online speed-up-my-PC services are using advanced network security algorithms. Look … we kill people with drones *every day* on the basis of Big Data. You think we've got handsome NCIS agents prowling the outskirts of Sana'a calling in air strikes on the bad guys? No, we've got terrestrial and low-orbit devices picking up a cell phone signal that our NSA Big Data Machine tells us is highly likely to be associated with a high value target, and then we send in a drone to go blow up whoever is holding the cellphone. Now say what you will about the morality of all this (my view: the NSA gives new meaning to what Hannah Arendt once called, in reference to Adolf Eichmann, "the banality of evil"), but don't tell me that the NSA is incompetent or doesn't know what it's doing. Big Data works.

Not sure I understand. "to identify the unique individual purchasing patterns of 90% of the people involved" … it doesn't say it identifies the people involved. It's a collection of purchasing patterns that belong to who knows.
-- "AF"

Sigh! Yet another article that starts with point A and leaps to point Doom. That algorithm doesn't identify the individual, all it does is look at the data and posit which transactions are likely to have been carried out by the same individual.
-- "R"

These comments illustrate a very common misconception about Big Data and the collection of "anonymous data", a misconception that is (surprise!) intentionally spread by the collectors of that data. For most Big Data purposes, nothing is gained by going the last mile to connect a specific name to a specific set of behaviors. To continue with the NSA example above, if I want to kill everyone in Yemen who has placed a cellphone call to a set of people who, in their aggregate behaviors, score high on some security threat matrix, then it would just slow me down to learn individual names. I'm going to kill whoever is holding that cellphone, regardless of what his name is. Or if you prefer a feel-good example, if I want to advertise my new movie to everyone who tweeted to a set of people who, in their aggregate behaviors, score high on some movie affinity matrix, then it would similarly just slow me down to learn individual names. But just because it's usually inefficient to infer a specific identity from the data doesn't mean it's not possible. Actually, it's child's play, and for those rare applications that require specific identities you don't stand a chance.

Ray Dalio's $165 billion Bridgewater Associates will start a new, artificial-intelligence unit next month with about half a dozen people, according to a person with knowledge of the matter. The team will report to David Ferrucci, who joined Bridgewater at the end of 2012 after leading the International Business Machines Corp. engineers that developed Watson, the computer that beat human players on the television quiz show "Jeopardy!"

The unit will create trading algorithms that make predictions based on historical data and statistical probabilities, said the person, who asked not to be identified because the information is private. The programs will learn as markets change and adapt to new information, as opposed to those that follow static instructions.

Quantitative investment firms including $24 billion Two Sigma Investments and $25 billion Renaissance Technologies are increasingly hiring programmers and engineers to expand their artificial-intelligence staffs.
-- Kelly Bit, "Bridgewater Is Said To Start Artificial-Intelligence Team", *Bloomberg*, Feb. 26, 2015

First, calling this "artificial intelligence" is a misnomer. There's nothing artificial about it. It's a non-human intelligence, but no less natural than our own. I dislike the term "artificial intelligence" because it implies that these systems are some sort of mimicry of the human brain, just on a larger, faster, more god-like scale. If you get nothing else out of what I've written on this subject (here and here), it's this: the inductive simultaneity of a powerful non-human intelligence is *sui generis*. It sees the world in an entirely different way than a human intelligence can, and in the right hands it is magic.

Second, everything I said above about "don't tell me that the NSA is incompetent or doesn't know what it's doing" … well, multiply that sentiment 10x when it comes to Bridgewater, Two Sigma, and Renaissance (and Citadel, and Fortress, and a dozen other firms I could name). What's possible here is

not only an accurate crystal ball for short-term market forecasts, but – even more profitably – the knowledge of what small market actions can trigger much larger market moves. Think of Ray Dalio standing on top of a giant mountain and rolling tiny snowballs down at you that get larger and larger as they pick up more snow. All completely legal. All completely above board. And all completely devastating. It's something that I've been working on for the past 4+ years, and I'm absolutely convinced it's possible. Within 20 years I don't think we will recognize public capital markets. They're going to be transformed by this technology into something else … a casino? a utility? … I have no idea where this goes. But it's going somewhere that will disrupt the current investment patterns and portfolios of trillions of dollars of capital. Good times.

And on that happy note I'll close this mailbag. Keep those cards and letters coming!

All the best,
Ben

To subscribe to Epsilon Theory:

- Sign up here: www.salientpartners.com/epsilontheory/subscribe
- **OR** send an email bhunt@salientpartners.com with your name, email address, and company affiliation (optional).

There is no charge to subscribe to Epsilon Theory and your email address will not be shared with anyone.

Follow me on Twitter: @EpsilonTheory

DISCLOSURES

This commentary is being provided to you by individual personnel of Salient Partners, L.P. and affiliates ("Salient") and is provided as general information only and should not be taken as investment advice. The opinions expressed in these materials represent the personal views of the author(s) and do not necessarily represent the opinions of Salient. It is not investment research or a research recommendation, as it does not constitute substantive research or analysis. Any action that you take as a result of information contained in this document is ultimately your responsibility. Salient will not accept liability for any loss or damage, including without limitation to any loss of profit, which may arise directly or indirectly from use of or reliance on such information. Consult your investment advisor before making any investment decisions. It must be noted, that no one can accurately predict the future of the market with certainty or guarantee future investment performance. Past performance is not a guarantee of future results.

Statements in this communication are forward-looking statements.
The forward-looking statements and other views expressed herein are as of the date of this publication. Actual future results or occurrences may differ significantly from those anticipated in any forward-looking statements, and there is no guarantee that any predictions will come to pass. The views expressed herein are subject to change at any time, due to numerous market and other factors. Salient disclaims any obligation to update publicly or revise any forward-looking statements or views expressed herein.

This information is neither an offer to sell nor a solicitation of any offer to buy any securities. Any offering or solicitation will be made only to eligible investors and pursuant to any applicable Private Placement Memorandum and other governing documents, all of which must be read in their entirety.

Salient commentary has been prepared without regard to the individual financial circumstances and objectives of persons who receive it. Salient recommends that investors independently evaluate particular investments and strategies, and encourage investors to seek the advice of a financial advisor. The appropriateness of a particular investment or strategy will depend on an investor's individual circumstances and objectives.

