Chain Follow
We build cryptographic ledgers that underpin breakthrough financial products
Oct 16 · 18 min read

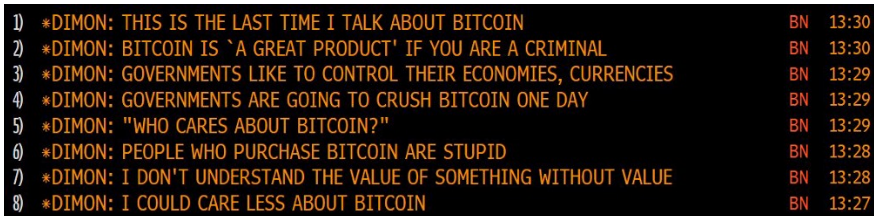
A Letter to Jamie Dimon

And anyone else still struggling to understand cryptocurrencies

Dear Jamie,

My name is Adam Ludwin and I run a company called Chain. I have been working in and around the cryptocurrency market for several years.

Last week you said a few things about Bitcoin:



```
1) *DIMON: THIS IS THE LAST TIME I TALK ABOUT BITCOIN                      BN  13:30
2) *DIMON: BITCOIN IS `A GREAT PRODUCT' IF YOU ARE A CRIMINAL              BN  13:30
3) *DIMON: GOVERNMENTS LIKE TO CONTROL THEIR ECONOMIES, CURRENCIES         BN  13:29
4) *DIMON: GOVERNMENTS ARE GOING TO CRUSH BITCOIN ONE DAY                  BN  13:29
5) *DIMON: "WHO CARES ABOUT BITCOIN?"                                      BN  13:29
6) *DIMON: PEOPLE WHO PURCHASE BITCOIN ARE STUPID                          BN  13:28
7) *DIMON: I DON'T UNDERSTAND THE VALUE OF SOMETHING WITHOUT VALUE         BN  13:28
8) *DIMON: I COULD CARE LESS ABOUT BITCOIN                                 BN  13:27
```

Bloomberg. https://twitter.com/joelight/status/918899226771427328

It’s easy to believe cryptocurrencies have no inherent value. Or that governments will crush them.

It’s also becoming fashionable to believe the opposite: that they will disrupt banks, governments, and Silicon Valley giants once and for all.

Neither extreme is true.

The reality is nuanced and important. Which is why I’ve decided to write you this briefing note. I hope it helps you appreciate cryptocurrencies more deeply.

Let me start by stating that I believe:

- The market for cryptocurrencies is overheated and irrationally exuberant

- There are a lot of poseurs creating them, and some scammers, too
- There are a lot of conflicts of interest, self-serving hype, and obfuscation
- Very few people in the media understand what's going on
- Very few people in finance understand what's going on
- Very few people in technology understand what's going on
- Very few people in academia or government understand what's going on
- Very few people *buying cryptocurrencies* understand what's going on
- It's very possible *I* don't understand what's going on

Also:

- Banks and governments aren't going away
- Traditional software isn't going away

In short: there's a lot of noise. But there is also signal. To find it, we need to start by *defining* cryptocurrency.

Without a working definition we are lost. Most people arguing about cryptocurrencies are talking past each other because they don't stop to ask the other side what they think cryptocurrencies are *for*.

Here's my definition: cryptocurrencies are a *new asset class* that enable *decentralized applications*.

If this is true, your point of view on cryptocurrencies has very little to do with what you think about them in comparison to traditional currencies or securities, and everything to do with your opinion of *decentralized applications and their value relative to current software models*.

Don't have an opinion on decentralized applications? Then you can't possibly have one on cryptocurrencies yet, so read on.

And since this isn't about cryptocurrencies vs. fiat currencies let's stop using the word *currency*. It's a head fake. It has way too much baggage and I notice that when you talk about Bitcoin in public you keep comparing it to the Dollar, Euro, and Yen. That comparison won't help you understand what's going on. In fact, it's getting in the way. So for the rest of this note, I will refer to cryptocurrencies as *crypto assets.*

So, to repeat: crypto assets are a *new asset class* that enable decentralized applications.

And like every other asset class, they exist as a mechanism to *allocate resources to a specific form of organization.* Despite the myopic focus on trading crypto assets recently, they don't exist solely to be traded. That is, in principle at least, they don't exist for their own sake.

To understand what I mean, think about other asset classes and what form of organization they serve:

- Corporate equities *serve* companies
- Government bonds *serve* nations, states, municipalities
- Mortgages *serve* property owners

And now:

- Crypto assets *serve* decentralized applications

Decentralized applications are a *new form of organization* and a *new form of software*. They're a new model for creating, financing, and operating software services in a way that is decentralized top-to-bottom. That doesn't make them *better* or *worse* than existing software models or the corporate entities that create them. As we'll see later, there are major trade-offs. What we can say is simply that they are *radically* different from software as we know it today and *radically* different from the forms of organization we are used to.

How different? Imagine the following: you grew up in a rainforest and I brought you a cactus and told you it was a tree. How would you react? You'd probably laugh and say it's not a tree because there's no point in a tree being a stumpy water tank covered in armor—after all, water is abundant here in the rainforest! This, roughly, is the reaction of many people working in Silicon Valley to decentralized applications.

But I digress. I owe you an important explanation:

What is a decentralized application?

A decentralized application is a way to create a service that no single entity operates.

We'll come to the question of *whether that's useful* in a moment. But first, you need to understand how they work.

Let's go back to the birth of this idea.

It's November 2008. The nadir of the financial crisis.

An anonymous person publishes a paper explaining how to make electronic payments without a trusted central party like Chase or PayPal or the Federal Reserve. It's the first *decentralized application* of this kind ever proposed.

It's a decentralized application *for payments*.

The paper is titled Bitcoin.

How does it work? How is it possible to send an electronic payment without a designated party who will track and update everyone's balances? If I hand you a dollar that's one thing. But data is not a bearer instrument. Data needs intermediation and validation to be trusted.

The paper proposes a solution: form a peer-to-peer network. Make it public. Announce your transaction to everyone. In your announcement, point to the specific funds on the network you want to spend. Cryptographically sign your announcement with the same software key that is linked to those funds so we know they're yours.

It almost works. We need one more thing: a way to make sure that if you broadcast two competing announcements (that is, if you try to spend the same funds twice) that only one of your attempts counts.

Bad solution: designate a party to timestamp the transactions and only include the transaction that came first. We're back to square one. We have a trusted intermediary.

Breakthrough solution: let entities compete to be the "timestamper!" We can't avoid the need for one, but we can avoid designating one in advance or using the same one for every batch of transactions.

"Let entities compete." Sounds like a market economy. What's missing? A reward for winning. An incentive. An asset.

Let's call that asset Bitcoin. Let's call the entities competing for the right to timestamp the latest batch of announced transactions "miners." Let's make sure anyone can join this contest at any time by making the code and network open.

Now we need an actual contest. The paper proposes one. On your mark, get set: find a random number generated by the network! The number is really, really hard to find. So hard that the only way to find it is to use tons of processing power and burn through electricity. It's a computing version of what Veruca Salt made her dad and his poor factory workers do in Willy Wonka. A brute force search for a golden ticket (or in this case, a golden number).

Veruca Salt's Golden Ticket

Bitcoin Mining

Why the elaborate and expensive competition to do something as simple as timestamp transactions for the network? So that we can be sure the competitors have incurred a *real financial cost*. That way, if they win the race to find the random number and become the designated timestamper for a given batch of transactions, they won't use that power for evil (like censoring transactions). Instead, they will meticulously scan each pending transaction, eliminate any attempts by users to spend the same funds twice, ensure all rules are followed, and broadcast the validated batch to the rest of the network.

Because if they do indeed follow the rules, the network is programmed to reward them…

… with newly minted Bitcoin, plus the transaction fees, denominated in Bitcoin, paid by the senders. (See why they are called *miners* and not *timestampers*, now?)

In other words, miners follow the rules because it is in their economic self-interest to do the right thing.

You know, like Adam Smith said:

> *It is not from the benevolence of the butcher, the brewer or the baker, that we expect our dinner, but from their regard to their own self interest.*

Crypto assets: the invisible hand… of the internet.

Bitcoin is capitalism, distilled. You should love it!

And since these miners have debts to pay (mostly electricity bills), they will likely sell their newly earned Bitcoins on the open market in exchange for whatever real currency they need to satisfy their liabilities. Anything left is profit. The Bitcoin is now in circulation. People who need it can buy it. And so can people who just want to speculate on it. (More on the people who "need it" vs. those who are speculating later.)

Eureka! We have killed two birds with one stone: the financial reward that substitutes our need for a trusted central party with a marketplace of competing yet honest timestampers *is the same asset* that ends up in circulation for use as a *digital bearer instrument* in an electronic payments network that has no central party (it's circular, I know).

Now that you understand Bitcoin, let's generalize this to decentralized applications as a whole.

In general, a decentralized application allows you to do something you can already do today (like payments) but without a trusted central party.

Here's another example: a decentralized application called Filecoin enables users to store files on a peer-to-peer network of computers instead of in centralized file storage services like Dropbox or Amazon S3. Its crypto asset, also called Filecoin, incentivizes entities to share excess hard drive space with the network.

Digital file storage is not new. Neither is electronic payments. What's new is that they can be operated *without a company*. A new form of organization.

One more example.

Warning: this one is a bit confusing because it's *meta*.

There's a decentralized application called Ethereum that is a *decentralized application for launching decentralized applications*. I am sure by now you have heard of "initial coin offerings" (ICOs) and "tokens." Most of these are issued on top of Ethereum. Instead of building a decentralized application from scratch the way Bitcoin was, you can build one on top of Ethereum much more easily because a) the network already exists and b) it's not designed for a *specific* application but rather as a platform to build applications that can execute arbitrary code. It is "featureless."

Ethereum's protocol incentivizes entities to contribute *computing resources* to the network. Doing so earns these entities Ether, the crypto asset of Ethereum. This makes Ethereum a new kind of computing platform for this new class of software (decentralized apps). It's not cloud computing because Ethereum itself is decentralized (like *aether*, get it?). That's why its founder, Vitalik Buterin, refers to Ethereum as a "world computer."

To summarize, in just the last few years the world has invented a way to create software services that have no central operator. These services are called decentralized applications and they are enabled with crypto assets that incentivize entities on the internet to contribute resources—processing, storage, computing—necessary for the service to function.

It’s worth pausing to acknowledge that this is kind of *miraculous*. With just the internet, an open protocol, and a new kind of asset, we can instantiate networks that dynamically assemble the resources necessary to provide many kinds of services.

And there are a lot of people who think this model is the *future of all software,* the thing that will finally challenge the FANG stocks and venture capital to boot.

But I’m not one of them. Because there’s a problem.

It’s not at all clear yet that decentralized applications are actually useful to most people relative to traditional software.

Simply put, you cannot argue that for *everyone* Bitcoin is *better* than PayPal or Chase. Or that for *everyone* Filecoin is *better* than Dropbox or iCloud. Or that for *everyone* Ethereum is *better* than Amazon EC2 or Azure.

In fact, on almost every dimension, decentralized services are *worse than their centralized counterparts:*

- They are slower
- They are more expensive
- They are less scalable
- They have worse user experiences
- They have volatile and uncertain governance

And no, this isn’t just because they are new. This won’t fundamentally change with bigger blocks, lightning networks, sharding, forks, self-amending ledgers, or any other technical solutions.

That’s because there are structural trade-offs that result directly from the primary design goal of these services, beneath which all other goals must be subordinated in order for them to be relevant: *decentralization.*

Remember that “elaborate and expensive competition” I described? Well, it comes at the cost of throughput. Remember how users need to “cryptographically sign” their transaction announcements? Well, those private keys need to be held onto much more securely than a typical password (passwords can be recovered). Remember how “no single entity operates” these networks? The flip side is that there is no good way to make decisions or govern them.

Sure, you can make decentralized applications more efficient and user friendly by, for example, centralizing users’ cryptographic signing keys (i.e., control of their coins) with a trusted entity. But then we’re mostly back to square one and would be better off using a service that is centralized.

Thus, bitcoin, for example, isn’t best described as “Decentralized PayPal.” It’s more honest to say it’s an extremely inefficient electronic payments network, *but in exchange we get decentralization.*

Bottom line: centralized applications beat the pants off decentralized applications on virtually every dimension.

EXCEPT FOR ONE DIMENSION.

And not only are decentralized applications better at this one thing, *they are the only way we can achieve it*.

What am I referring to?

Censorship resistance.

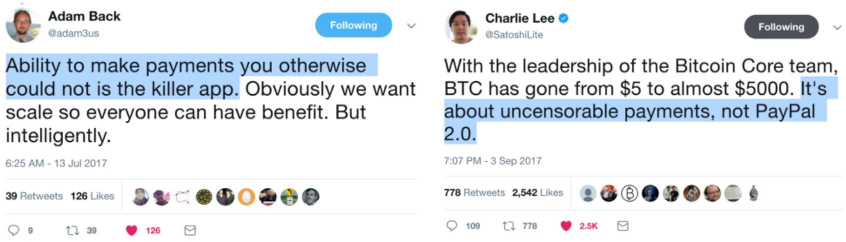
This is where we come to the elusive signal in the noise.

Censorship resistance means that access to decentralized applications is open and unfettered. Transactions on these services are *unstoppable*.

More concretely, nothing can stop me from sending Bitcoin to anyone I please. Nothing can stop me from executing code on Ethereum. Nothing can stop me from storing files on Filecoin. As long as I have an internet connection and pay the network’s transaction fee, denominated in its crypto asset, I am free to do what I want.

(If Bitcoin is capitalism distilled, it’s also a kind of freedom distilled. Which is why libertarians can get a bit obsessed.)

And for readers who are crypto enthusiasts and don’t want to take my word for it, will you at least listen to Adam Back and Charlie Lee?



Adam Back
@adam3us
Following

Ability to make payments you otherwise could not is the killer app. Obviously we want scale so everyone can have benefit. But intelligently.

6:25 AM - 13 Jul 2017

39 Retweets 126 Likes

9 39 126

Charlie Lee
@SatoshiLite
Following

With the leadership of the Bitcoin Core team, BTC has gone from $5 to almost $5000. It's about uncensorable payments, not PayPal 2.0.

7:07 PM - 3 Sep 2017

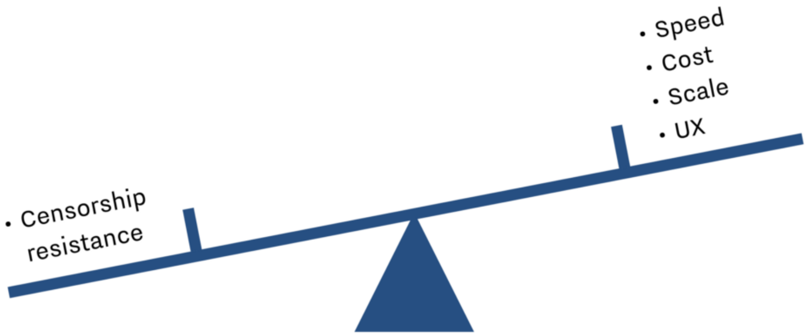
778 Retweets 2,542 Likes

109 778 2.5K

So while we can’t say “for everyone Bitcoin is better than Visa,” it is possible that *for some cohort of users* Bitcoin truly is the only way to make a payment.

More generally, we can ask:

For whom is this the right trade-off?



Who needs censorship resistance so much that they are willing to trade away the speed, cost, scalability, and experience benefits of centralized services?

To be clear, I’m not saying you have to make this trade-off *in order to buy/speculate on crypto assets*. I am saying that in order for decentralized applications themselves to have utility to some cohort, that cohort must be optimizing for censorship resistance.

So, who are these people?

While there is not a lot of good data, actual *users* of decentralized applications seem to fall into two categories:

1. People who are off the grid: that is, in countries where access to competently operated traditional services is limited (for any number of reasons) but where internet is not
2. People who *want to be* off the grid: that is, people who don't want their transactions censored or known

With that framework in mind we can ask:

- For whom is Bitcoin the best/only way to make a payment?
- For whom is Filecoin the best/only way to store a file?
- For whom is Ethereum the best/only way to compute code?

These are the questions that get at the heart of the value proposition of the technology.

So far, most decentralized applications have very little use relative to traditional services. Bitcoin, for example, has fewer mainstream merchants accepting it as a payment option in the U.S. today than in 2014. And for all the talk of Bitcoin's value as a payments system in developing countries or emerging markets like China, it is traditional software (i.e., apps) like AliPay and Paytm that are actually driving sweeping change in these places.

At the same time, use of Bitcoin on the dark web and for ransomware is evident, even if it is hard to get good data.

But aren't people using Bitcoin as a "store of value?" Sure, which is just another way of saying people are investing in Bitcoin with a longish time horizon. But remember I'm not talking about investing in the crypto asset yet. I'm talking about whether there are people who find a *decentralized application for payments* (which is enabled by that asset) useful. Real estate is only a good store of value *in the long run* if people live and work in the buildings. The same is true of decentralized applications.

What should we make of Ethereum evaluated through the "censorship resistance" lens? After all, it seems to be getting a ton of use by developers. Since Ethereum is a *developer platform for decentralized applications*, does that mean it is *developers* who have been censored or blocked somehow? In a way, yes. Developers and start-ups who wish to build financial products do not have open and unfettered access to the world's financial infrastructure. While Ethereum doesn't provide access to that infrastructure, it does provide a different infrastructure that can be used to, for example, create and execute a financial contract.

Since Ethereum is a platform, its value is ultimately a function of the value of the applications built on top. In other words, we can ask if Ethereum is useful by simply asking if anything that has been built on Ethereum is useful. For example, do we need censorship resistant prediction markets? Censorship resistant meme playing cards? Censorship resistant versions of YouTube or Twitter?

While it's early, if none of the 730+ decentralized apps built on Ethereum so far seem useful, that may be telling. Even in year 1 of the web we had chat rooms, email, cat photos, and sports scores. What are the equivalent killer applications on Ethereum today?

So where does this leave us?

Given how different they are from the app models we know and love, will anyone *ever really use* decentralized applications? Will they become a critical part of the economy? It's hard to predict because it depends in part on the technology's evolution but far more on society's reaction to it.

For example: until relatively recently, encrypted messaging was only used by hackers, spies, and paranoids. That didn't seem to be changing. Until it did. Post-Snowden and post-Trump, everyone from Silicon Valley to the Acela corridor seems to be on either Signal or Telegram. WhatsApp is end-to-end encrypted. The press solicit tips through SecureDrop. Yes, the technology got a little better and easier to use. But it is mainly changes in society that are driving adoption.

In other words, we grew up in the rainforest, but sometimes things change and it helps to know how to adapt to other environments.

And this is the basic argument that the smart money is making on crypto assets and decentralized applications: that it's simply too early to say anything. That it is a profound change. That, should one or more of these decentralized applications actually become an integral part of the world, their underlying crypto assets will be extremely valuable. So might as well start placing bets now and see how it goes. Don't get to hung up on whether we see the killer apps yet.

That's not a bad argument and I tend to agree.

I would summarize the argument as: in the long-run, a crypto asset's value is driven by use of the decentralized application it enables. While it's early, the high valuations are justified because even if the probability of mass adoption is small, the impact would be very large, so might as well go along for the ride and see what happens.

But how do we explain the recent mania?

Bitcoin is up 5x in a year, Ethereum is up 30x. The total market cap of all cryptocurrencies is ~$175B, up from $12B just a year ago. Why?

As in every mania in history, it is currently rational to be irrational.

To understand what's going on, let's look at the buyer and seller mentality right now, starting with the buyers.

If you invested early in Bitcoin or Ethereum, you are sitting on a windfall. It feels like you are playing with "house money," a well-known psychological effect. You feel smart and willing to risk more than you otherwise would if it was "your money." Might as well diversify a bit and parlay your gains into the next crypto asset, or two, or three.

If you *didn't* invest, the fear-of-missing-out continues to build until the "screw it" moment when you buy in. Maybe you read about Bitcoin, didn't understand it, and followed Warren Buffet's (good) advice not to invest in things you don't understand. Some of your friends made money but you still ignored it. Then you read about Ethereum, which you *really* didn't understand, also passed on buying, and later found out that your friends are planning to retire because they did. The lesson seems to be *anti-Buffet*: only invest in things you *don't understand*. This is causing people to check their judgement at the door when the latest all-time high finally convinces them to jump into the market.

And that is not good.

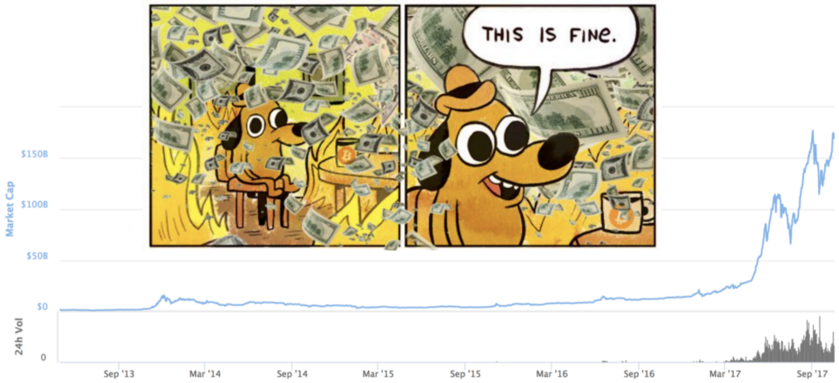
Because there will be sellers to fill the demand, especially the demand coming from people who have decided they will never understand this stuff so will just place bets on things that *sound complex and impressive.*

Let's think about these sellers. And by sellers, I don't mean people selling their holdings of existing crypto assets. I mean new issuers. Teams launching new crypto assets.

The basic model is to pre-sell some percentage of the crypto assets the proposed network will generate as a way to fund the development of the decentralized application before it launches. The project founders tend to hold on to some percentage of these assets. Which means that raising money for a project this way is a) non-dilutive as it is not equity and b) not debt, so you never have to pay anyone back. This is basically free money. It's never been this good for entrepreneurs, even in the 90s dot-com boom. Which makes it incredibly tempting to try and shoe-horn every project that *could perhaps* justify an "initial coin offering" to go for it, even if they aren't actually building a *decentralized* application. After all, an ICO lets you exit before you even launch.

And there is a pervasive narrative out there that supports entrepreneurs looking to create new crypto assets. The idea is that by selling assets to users before your network launches, you create "evangelists" who will be early users and promoters you wouldn't otherwise have if there were no financial incentive to participate in your community.

The problem with this line of thinking is that it conflates early *investors* with early *users.* The overlap between people who buy your crypto asset and people who actually want to use the service you are building is likely very, very small, especially during market manias like this one. It creates a false sense of "product-market fit." Yes, people are buying your crypto asset. But that's because the "market" are people who want to get rich and the "product" you are selling is a "way to get rich."



But "this is fine."

Everyone's making money. For now.

It's currently rational to be irrational.

As long as that blue line keeps going up.

> *Only when the tide goes out do you discover who's been swimming naked.*

At the same time, I wouldn't bet against crypto assets.

> *He who lives by the crystal ball will eat shattered glass.*

Consider the following. The total market cap of crypto assets has been increasing by an *order of magnitude* every few years. Where will they be in 2022? It's certain that many (most?) of the crypto assets launching today won't make it. But neither did most of the ones that were launched back in the 2013/4 boom (when they were referred to as "alt coins"). Though an important alt coin from 2014 did stick around and drove the most recent boom to new heights by being the platform to power all the others: Ethereum.

2008	2011	2013	2017	2022
0 Mkt Cap	0.1 bn Mkt Cap	10 bn Mkt Cap	100 bn Mkt Cap	??? Mkt Cap

So, Jamie, what's the bottom line?

Allow me to summarize.

- Cryptocurrencies (which I prefer to call crypto assets) are a new asset class that enable decentralized applications
- Decentralized applications enable services we already have today, like payments, storage, or computing, but without a central operator of those services
- This software model is useful to people who need censorship resistance which tend to be people that are either off the grid or who want to be off the grid
- Most everyone else is better off using normal applications because they are 10x better on every other dimension, at least for now
- Society's embrace or rejection of new technology is hard to predict (think about encrypted messaging)
- In the long-run, the value of a crypto asset will rise and fall in proportion to the use of the decentralized application it enables
- In the short-run, there will be extreme volatility as FOMO competes with FUD, confusion competes with understanding, and greed competes with fear (on both the buyer side and the issuer side)
- Most people buying into crypto assets have checked their judgement at the door
- Many sellers of new crypto assets aren't actually building decentralized applications but are instead shoe-horning an ICO into their service because of the market mania; that doesn't mean decentralized applications are bad, it just means people are capitalizing on the confusion and are probably themselves confused
- Don't bet against crypto assets in the long-run: as we approach the 10 year anniversary of the Bitcoin paper it is clear that they aren't going anywhere and that decentralized applications may very well find an important place alongside all the other forms of organization we have come to take for granted.

Best,
Adam

p.s. —You may have noticed that I didn't use the word "blockchain" in this note. The word now tends to confuse more than enlighten.

p.p.s—There is another, related market I didn't talk about: cryptographic ledgers for the enterprise. My perspective on that is here.