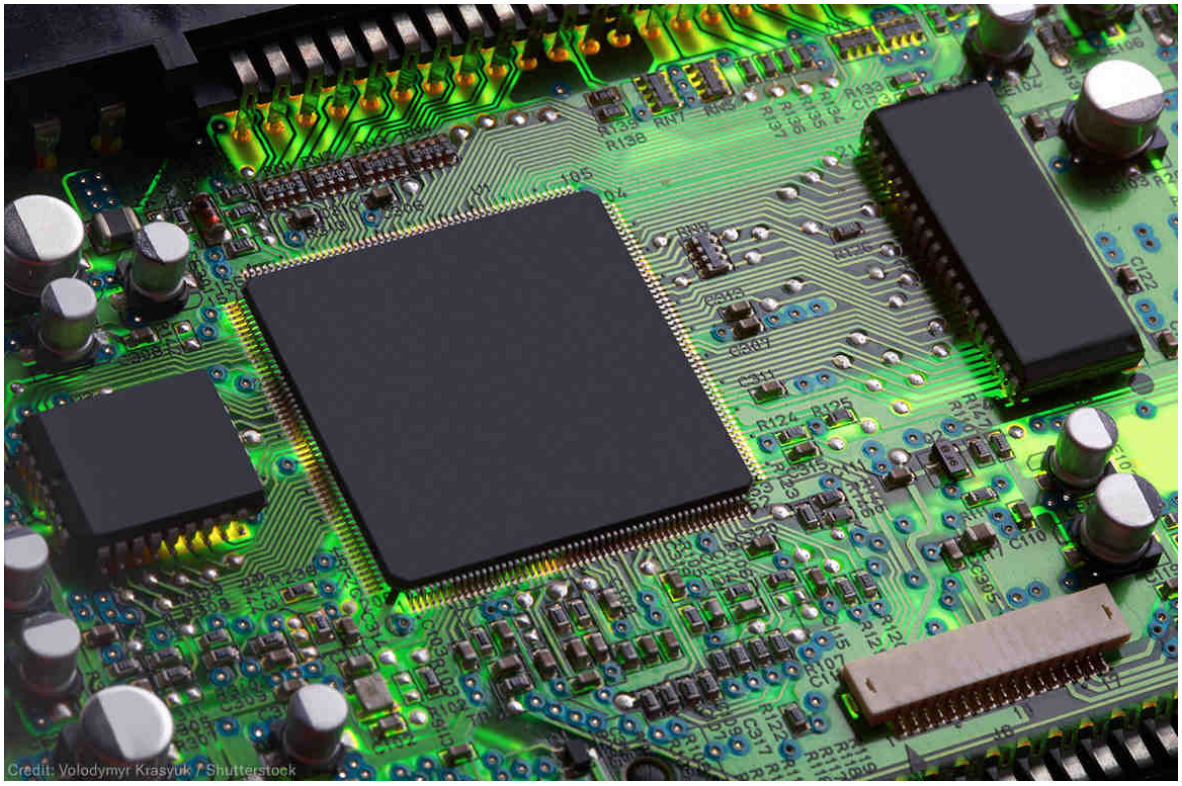
ACLU 100 YEARS

FREE FUTURE

# Edward Snowden Explains Blockchain to His Lawyer — and the Rest of Us

By Ben Wizner, Director, ACLU Speech, Privacy, and Technology Project
NOVEMBER 20, 2018 | 3:30 PM

TAGS: Internet Privacy, Privacy & Technology




*[This piece originally appeared in McSweeney's new issue, The End of Trust, a collection featuring over 30 writers investigating surveillance, technology, and privacy, with special advisors the Electronic Frontier Foundation.]*

*Over the last five years, Edward Snowden and I have carried on an almost daily conversation, most of it unrelated to his legal troubles. Sometimes we meet in person in Moscow over vodka (me) and milkshakes (him). But our friendship has mostly taken place on secure messaging platforms, a channel that was comfortable and intuitive for him but took some getting used to for me. I learned to type with two thumbs as we discussed politics, law, and literature; family, friends, and foster dogs. Our sensibilities are similar but our worldviews quite different: I sometimes accuse him of technological solutionism; he accuses me of timid incrementalism.*

*Through it all, I've found him to be the clearest, most patient, and least condescending explainer of technology I've ever met. I've often thought that I wished more people – or perhaps different people – could eavesdrop on our conversations. What follows is a very lightly edited transcript of one of our chats. In it, Ed attempts to explain "blockchain" to me, despite my best efforts to cling to my own ignorance.*

**Ben Wizner:** The Electronic Frontier Foundation recently joked that "the amount of energy required to download tweets, articles, and instant messages which describe what 'the blockchain' is and how 'decentralized' currencies are 'the future' will soon eclipse the total amount of power used by the country of Denmark." It's true that there are a lot of "blockchain explainers" out there. And yet I'm ashamed to admit I still don't really get it.

**Edward Snowden:** Are you asking for another math lesson? I've been waiting for this day. You remember what a cryptographic hash function is, right?

**BW:** This is where I'm supposed to make a joke about drugs. But no, I do not now nor will I ever remember that.

**ES:** Challenge accepted. Let's start simpler: what do you know about these mythical blockchains?

**BW:** That I could have been rich if I'd listened to you about this four years ago? But really, I've heard a lot and understood little. "Decentralized." "Ledgers." What the hell is a blockchain?

**ES:** It's basically just a new kind of database. Imagine updates are always added to the end of it instead of messing with the old, preexisting entries — just as you could add new links to an old chain to make it longer — and you're on the right track. Start with that concept, and we'll fill in the details as we go.

**BW:** Okay, but why? What is the question for which blockchain is the answer?

**ES:** In a word: trust. Imagine an old database where any entry can be changed just by typing over it and clicking save. Now imagine that entry holds your bank balance. If somebody can just arbitrarily change your balance to zero, that kind of sucks, right? Unless you've got student loans.

The point is that any time a system lets somebody change the history with a keystroke, you have no choice but to trust a huge number of people to be both perfectly good and competent, and humanity doesn't have a great track record of that. Blockchains are an effort to create a history that can't be manipulated.

**BW:** A history of what?

**ES:** Transactions. In its oldest and best-known conception, we're talking about Bitcoin, a new form of money. But in the last few months, we've seen efforts to put together all kind of records in these histories. Anything that needs to be memorialized and immutable. Health-care records, for example, but also deeds and contracts.

When you think about it at its most basic technological level, a blockchain is just a fancy way of time-stamping things in a manner that you can prove to posterity hasn't been tampered with after the fact. The very first bitcoin ever

created, the "Genesis Block," famously has one of those "general attestations" attached to it, which you can still view today.

It was a cypherpunk take on the old practice of taking a selfie with the day's newspaper, to prove this new bitcoin blockchain hadn't secretly been created months or years earlier (which would have let the creator give himself an unfair advantage in a kind of lottery we'll discuss later).

**BW:** Blockchains are a history of transactions. That's such a letdown. Because I've heard some extravagant claims like: blockchain is an answer to censorship. Blockchain is an answer to online platform monopolies.

**ES:** Some of that is hype cycle. Look, the reality is blockchains can theoretically be applied in many ways, but it's important to understand that mechanically, we're discussing a very, very simple concept, and therefore the applications are all variations on a single theme: verifiable accounting. Hot.

So, databases, remember? The concept is to bundle up little packets of data, and that can be anything. Transaction records, if we're talking about money, but just as easily blog posts, cat pictures, download links, or even moves in the world's most over-engineered game of chess. Then, we stamp these records in a complicated way that I'm happy to explain despite protest, but if you're afraid of math, you can think of this as the high-tech version of a public notary. Finally, we distribute these freshly notarized records to members of the network, who verify them and update their independent copies of this new history. The purpose of this last step is basically to ensure no one person or small group can fudge the numbers, because too many people have copies of the original.

It's this decentralization that some hope can provide a new lever to unseat today's status quo of censorship and entrenched monopolies. Imagine that instead of today's world, where publicly important data is often held exclusively at GenericCorp LLC, which can and does play God with it at the public's expense, it's in a thousand places with a hundred jurisdictions. There is no takedown mechanism or other "let's be evil" button, and creating one

requires a global consensus of, generally, at least 51 percent of the network in support of changing the rules.

**mechanically, we're discussing a very, very simple concept, and therefore the applications are all variations on a single theme: verifiable accounting. Hot.**

**BW:** So even if Peter Thiel won his case and got a court order that some article about his vampire diet had to be removed, there would be no way to enforce it. Yes? That is, if *Blockchain Magazine* republished it.

**ES:** Right — so long as *Blockchain Magazine* is publishing to a decentralized, public blockchain, they could have a judgment ordering them to set their office on fire and it wouldn't make a difference to the network.

**BW:** So... how does it work?

**ES:** Oh man, I was waiting for this. You're asking for the fun stuff. Are you ready for some abstract math?

**BW:** As ready as I'll ever be.

**ES:** Let's pretend you're allergic to finance, and start with the example of an imaginary blockchain of blog posts instead of going to the normal Bitcoin examples. The interesting mathematical property of blockchains, as mentioned earlier, is their general immutability a very short time past the point of initial publication.

For simplicity's sake, think of each new article published as representing a "block" extending this blockchain. Each time you push out a new article, you are adding another link to the chain itself. Even if it's a correction or update to an old article, it goes on the end of the chain, erasing nothing. If your chief concerns were manipulation or censorship, this means once it's up, it's up. It is practically impossible to remove an earlier block from the chain without also destroying every block that was created after that point and convincing

everyone else in the network to agree that your alternate version of the history is the correct one.

Let's take a second and get into the reasons for why that's hard. So, blockchains are record-keeping backed by fancy math. Great. But what does that mean? What actually stops you from adding a new block somewhere other than the end of the chain? Or changing one of the links that's already there?

We need to be able to crystallize the things we're trying to account for: typically a record, a timestamp, and some sort of proof of authenticity.

So on the technical level, a blockchain works by taking the data of the new block — the next link in the chain — stamping it with the mathematic equivalent of a photograph of the block immediately preceding it and a timestamp (to establish chronological order of publication), then "hashing it all together" in a way that proves the block qualifies for addition to the chain.

**BW:** "Hashing" is a real verb?

**ES:** A cryptographic hash function is basically just a math problem that transforms any data you throw at it in a predictable way. Any time you feed a hash function a particular cat picture, you will always, always get the same number as the result. We call that result the "hash" of that picture, and feeding the cat picture into that math problem "hashing" the picture. The key concept to understand is that if you give the very same hash function a slightly different cat picture, or the same cat picture with even the tiniest modification, you will get a WILDLY different number ("hash") as the result.

**BW:** And you can throw any kind of data into a hash function? You can hash a blog post or a financial transaction or *Moby-Dick*?

**ES:** Right. So we hash these different blocks, which, if you recall, are just glorified database updates regarding financial transactions, web links, medical records, or whatever. Each new block added to the chain is identified and

validated by its hash, which was produced from data that intentionally includes the hash of the block before it. This unbroken chain leads all the way back to the very first block, which is what gives it the name.

I'm sparing you some technical nuance here, but the important concepts to understand are that blocks in the chain are meant to be verifiable, strictly ordered by chronology, and immutable. Each new block created, which in the case of Bitcoin happens every ten minutes, effectively testifies about the precise contents of all the ones that came before it, making older blocks harder and harder to change without breaking the chain completely.

So by the time our Peter Thiel catches wind of the story and decides to kill it, the chain has already built a thousand links of confirmable, published history.

## Money is, of course, the best and most famous example of where blockchains have been proven to make sense.

**BW:** And this is going to... save the internet? Can you explain why some people think blockchain is a way to get around or replace huge tech platform monopolies? Like how could it weaken Amazon? Or Google?

**ES:** I think the answer there is "wishful thinking." At least for the foreseeable future. We can't talk Amazon without getting into currency, but I believe blockchains have a much better chance of disrupting trade than they do publication, due to their relative inefficiency.

Think about our first example of your bank balance in an old database. That kind of setup is fast, cheap, and easy, but makes you vulnerable to the failures or abuses of what engineers call a "trusted authority." Blockchains do away with the need for trusted authorities at the expense of efficiency. Right now, the old authorities like Visa and MasterCard can process tens of thousands of transactions a second, while Bitcoin can only handle about seven. But methods of compensating for that efficiency disadvantage are being worked on, and we'll see transaction rates for blockchains improve in the next few years to a point where they're no longer a core concern.

**BW:** I've been avoiding this, because I can't separate cryptocurrency from the image of a bunch of tech bros living in a palace in Puerto Rico as society crumbles. But it's time for you to explain how Bitcoin works.

**ES:** Well, I hate to be the bearer of bad news, but Zuckerberg is already rich.

Money is, of course, the best and most famous example of where blockchains have been proven to make sense.

**BW:** With money, what is the problem that blockchain solves?

**ES:** The same one it solves everywhere else: trust. Without getting too abstract: what *is* money today? A little cotton paper at best, right? But most of the time, it's just that entry in a database. Some bank says you've got three hundred rupees today, and you really hope they say the same or better tomorrow.

Now think about access to that reliable bank balance — that magical number floating in the database — as something that can't be taken for granted, but is instead transient. You're one of the world's unbanked people. Maybe you don't meet the requirements to have an account. Maybe banks are unreliable where you live, or, as happened in Cyprus not too long ago, they decided to seize people's savings to bail themselves out. Or maybe the money itself is unsound, as in Venezuela or Zimbabwe, and your balance from yesterday that could've bought a house isn't worth a cup of coffee today. Monetary systems fail.

**BW:** Hang on a minute. Why is a "bitcoin" worth anything? What generates value? What backs the currency? When I own a bitcoin, what do I really own?

**ES:** Good question. What makes a little piece of green paper worth anything? If you're not cynical enough to say "men with guns," which are the reason legal tender is treated different from Monopoly money, you're talking about scarcity and shared belief in the usefulness of the currency as a store of value or a means of exchange.

Let's step outside of paper currencies, which have no fundamental value, to a more difficult case: why is gold worth so much more than its limited but real practical uses in industry? Because people generally agree it's worth more than its practical value. That's really it. The social belief that it's expensive to dig out of the ground and put on a shelf, along with the expectation that others are also likely to value it, transforms a boring metal into the world's oldest store of value.

Blockchain-based cryptocurrencies like Bitcoin have very limited fundamental value: at most, it's a token that lets you save data into the blocks of their respective blockchains, forcing everybody participating in that blockchain to keep a copy of it for you. But the scarcity of at least some cryptocurrencies is very real: as of today, no more than twenty-one million bitcoins will ever be created, and seventeen million have already been claimed. Competition to "mine" the remaining few involves hundreds of millions of dollars' worth of equipment and electricity, which economists like to claim are what really "backs" Bitcoin.

Yet the hard truth is that the only thing that gives cryptocurrencies value is the belief of a large population in their usefulness as a means of exchange. That belief is how cryptocurrencies move enormous amounts of money across the world electronically, without the involvement of banks, every single day. One day capital-B Bitcoin will be gone, but as long as there are people out there who want to be able to move money without banks, cryptocurrencies are likely to be valued.

**BW:** But what about you? What do you like about it?

**ES:** I like Bitcoin transactions in that they are impartial. They can't really be stopped or reversed, without the explicit, voluntary participation by the people involved. Let's say Bank of America doesn't want to process a payment for someone like me. In the old financial system, they've got an enormous amount of clout, as do their peers, and can make that happen. If a teenager in Venezuela wants to get paid in a hard currency for a web development gig they did for someone in Paris, something prohibited by local currency

controls, cryptocurrencies can make it possible. Bitcoin may not yet really be private money, but it is the first "free" money.

Bitcoin has competitors as well. One project, called Monero, tries to make transactions harder to track by playing a little shell game each time anybody spends money. A newer one by academics, called Zcash, uses novel math to enable truly private transactions. If we don't have private transactions by default within five years, it'll be because of law, not technology.

**As with all new technologies, there will be disruption and there will be abuse. The question is whether, on balance, the impact is positive or negative.**

**BW:** So if Trump tried to cut off your livelihood by blocking banks from wiring your speaking fees, you could still get paid.

**ES:** And all he could do is tweet about it.

**BW:** The downside, I suppose, is that sometimes the ability of governments to track and block transactions is a social good. Taxes. Sanctions. Terrorist finance.

We want you to make a living. We also want sanctions against corrupt oligarchs to work.

**ES:** If you worry the rich can't dodge their taxes without Bitcoin, I'm afraid I have some bad news. Kidding aside, this is a good point, but I think most would agree we're far from the low-water mark of governmental power in the world today. And remember, people will generally have to convert their magic internet money into another currency in order to spend it on high-ticket items, so the government's days of real worry are far away.

**BW:** Explore that for me. Wouldn't the need to convert Bitcoin to cash also affect your Venezuelan teen?

**ES:** The difference is scale. When a Venezuelan teen wants to trade a month's wages in cryptocurrency for her local currency, she doesn't need an ID check and a bank for that. That's a level of cash people barter with every day, particularly in developing economies. But when a corrupt oligarch wants to commission a four hundred million-dollar pleasure yacht, well, yacht builders don't have that kind of liquidity, and the existence of invisible internet money doesn't mean cops won't ask how you paid for it.

The off-ramp for one is a hard requirement, but the other can opt for a footpath.

Similarly, it's easier for governments to work collectively against "real" criminals — think bin Laden — than it is for them to crack down on dissidents like Ai Weiwei. The French would work hand in hand with the Chinese to track the activity of bin Laden's Bitcoin wallet, but the same is hopefully not true of Ai Weiwei.

**BW:** So basically you're saying that this won't really help powerful bad actors all that much.

**ES:** It could actually hurt them, insofar as relying on blockchains will require them to commit evidence of their bad deeds onto computers, which, as we've learned in the last decade, government investigators are remarkably skilled at penetrating.

**BW:** How would you describe the downsides, if any?

**ES:** As with all new technologies, there will be disruption and there will be abuse. The question is whether, on balance, the impact is positive or negative. The biggest downside is inequality of opportunity: these are new technologies that are not that easy to use and still harder to understand. They presume access to a level of technology, infrastructure, and education that is not universally available. Think about the disruptive effect globalization has had on national economies all over the world. The winners have won by miles, not

inches, with the losers harmed by the same degree. The first-mover advantage for institutional blockchain mastery will be similar.

**BW:** And the internet economy has shown that a platform can be decentralized while the money and power remain very centralized.

**ES:** Precisely. There are also more technical criticisms to be made here, beyond the scope of what we can reasonably get into. Suffice it to say cryptocurrencies are normally implemented today through one of two kinds of lottery systems, called "proof of work" and "proof of stake," which are a sort of necessary evil arising from how they secure their systems against attack. Neither is great. "Proof of work" rewards those who can afford the most infrastructure and consume the most energy, which is destructive and slants the game in favor of the rich. "Proof of stake" tries to cut out the environmental harm by just giving up and handing the rich the reward directly, and hoping their limitless, rent-seeking greed will keep the lights on. Needless to say, new models are needed.

**BW:** Say more about the environmental harms. Why does making magical internet money use so much energy?

**ES:** Okay, imagine you decide to get into "mining" bitcoins. You know there are a limited number of them up for grabs, but they're coming from somewhere, right? And it's true: new bitcoins will still continue to be created every ten minutes for the next couple years. In an attempt to hand them out fairly, the original creator of Bitcoin devised an extraordinarily clever scheme: a kind of global math contest. The winner of each roughly ten-minute round gets that round's reward: a little treasure chest of brand new, never-used bitcoins, created from the answer you came up with to that round's math problem. To keep all the coins in the lottery from being won too quickly, the difficulty of the next math problem is increased based on how quickly the last few were solved. This mechanism is the explanation of how the rounds are always roughly ten minutes long, no matter how many players enter the competition.

The flaw in all of this brilliance was the failure to account for Bitcoin becoming too successful. The reward for winning a round, once worth mere pennies, is now around one hundred thousand dollars, making it economically reasonable for people to divert enormous amounts of energy, and data centers full of computer equipment, toward the math — or "mining" — contest. Town-sized Godzillas of computation are being poured into this competition, ratcheting the difficulty of the problems beyond comprehension.

This means the biggest winners are those who can dedicate tens of millions of dollars to solving a never-ending series of problems with no meaning beyond mining bitcoins and making its blockchain harder to attack.

**BW:** "A never-ending series of problems with no meaning" sounds like... nihilism. Let's talk about the bigger picture. I wanted to understand blockchains because of the ceaseless hype. Some governments think that Bitcoin is an existential threat to the world order, and some venture-capital types swear that blockchains will usher in a golden age of transparency. But you're telling me it's basically a fancy database.

**ES:** The tech is the tech, and it's basic. It's the applications that matter. The real question is not "what is a blockchain," but "how can it be used?" And that gets back to what we started on: trust. We live in a world where everyone is lying about everything, with even ordinary teens on Instagram agonizing over how best to project a lifestyle they don't actually have. People get different search results for the same query. Everything requires trust; at the same time nothing deserves it.

This is the one interesting thing about blockchains: they might be that one tiny gear that lets us create systems you don't have to trust. You've learned the only thing about blockchains that matters: they're boring, inefficient, and wasteful, but, if well designed, they're practically impossible to tamper with. And in a world full of shifty bullshit, being able to prove something is true is a radical development. Maybe it's the value of your bank account, maybe it's the provenance of your pair of Nikes, or maybe it's your for-real-this-time permanent record in the principal's office, but records are going to transform

into chains we can't easily break, even if they're open for anyone in the world to look at.

The hype is a world where everything can be tracked and verified. The question is whether it's going to be voluntary.

**BW:** That got dark fast. Are you optimistic about how blockchains are going to be used once we get out of the experimental phase?

**ES:** What do you think?



## RELATED STORIES


ACLU Calls On Tech Companies to End Their Alliance with ICE and CBP

SEPTEMBER 9, 2020

Maine's ISP Privacy Law Does Not Violate the First Amendment, Much as ISPs...

MAY 29, 2020

## STAY INFORMED