The New York Times Magazine | https://nyti.ms/2FGVArL

Beyond the Bitcoin Bubble

Yes, it's driven by greed and hubris and the mania for cryptocurrency. But the blockchain could wind up building something much more important than wealth.

By STEVEN JOHNSON JAN. 16, 2018

layer innocent nothing argue pottery winner cotton menu task slim merge maid

The sequence of words is meaningless: a random array strung together by an algorithm let loose in an English dictionary. What makes them valuable is that they've been generated exclusively for me, by a software tool called MetaMask. In the lingo of cryptography, they're known as my seed phrase. They might read like an incoherent stream of consciousness, but these words can be transformed into a key that unlocks a digital bank account, or even an online identity. It just takes a few more steps.

On the screen, I'm instructed to keep my seed phrase secure: Write it down, or keep it in a secure place on your computer. I scribble the 12 words onto a notepad, click a button and my seed phrase is transformed into a string of 64 seemingly patternless characters:

1b0be2162cedb2744d016943bb14e71de6af95a63af3790d6b41b1e719dc5c66

This is what's called a "private key" in the world of cryptography: a way of proving identity, in the same, limited way that real-world keys attest to your identity when you unlock your front door. My seed phrase will generate that exact sequence

of characters every time, but there's no known way to reverse-engineer the original phrase from the key, which is why it is so important to keep the seed phrase in a safe location.

That private key number is then run through two additional transformations, creating a new string:

0x6c2ecd6388c550e8d99ada34a1cd55bedd052ad9

That string is my address on the Ethereum blockchain.

Ethereum belongs to the same family as the cryptocurrency Bitcoin, whose value has increased more than 1,000 percent in just the past year. Ethereum has its own currencies, most notably Ether, but the platform has a wider scope than just money. You can think of my Ethereum address as having elements of a bank account, an email address and a Social Security number. For now, it exists only on my computer as an inert string of nonsense, but the second I try to perform any kind of transaction — say, contributing to a crowdfunding campaign or voting in an online referendum — that address is broadcast out to an improvised worldwide network of computers that tries to verify the transaction. The results of that verification are then broadcast to the wider network again, where more machines enter into a kind of competition to perform complex mathematical calculations, the winner of which gets to record that transaction in the single, canonical record of every transaction ever made in the history of Ethereum. Because those transactions are registered in a sequence of "blocks" of data, that record is called the blockchain.

The whole exchange takes no more than a few minutes to complete. From my perspective, the experience barely differs from the usual routines of online life. But on a technical level, something miraculous is happening — something that would have been unimaginable just a decade ago. I've managed to complete a secure transaction without any of the traditional institutions that we rely on to establish trust. No intermediary brokered the deal; no social-media network captured the data from my transaction to better target its advertising; no credit bureau tracked the activity to build a portrait of my financial trustworthiness.

And the platform that makes all this possible? No one owns it. There are no venture investors backing Ethereum Inc., because there is no Ethereum Inc. As an organizational form, Ethereum is far closer to a democracy than a private corporation. No imperial chief executive calls the shots. You earn the privilege of helping to steer Ethereum's ship of state by joining the community and doing the work. Like Bitcoin and most other blockchain platforms, Ethereum is more a swarm than a formal entity. Its borders are porous; its hierarchy is deliberately flattened.

Oh, one other thing: Some members of that swarm have already accumulated a paper net worth in the billions from their labors, as the value of one "coin" of Ether rose from $8 on Jan. 1, 2017, to $843 exactly one year later.

You may be inclined to dismiss these transformations. After all, Bitcoin and Ether's runaway valuation looks like a case study in irrational exuberance. And why should you care about an arcane technical breakthrough that right now doesn't feel all that different from signing in to a website to make a credit card payment?

But that dismissal would be shortsighted. If there's one thing we've learned from the recent history of the internet, it's that seemingly esoteric decisions about software architecture can unleash profound global forces once the technology moves into wider circulation. If the email standards adopted in the 1970s had included public-private key cryptography as a default setting, we might have avoided the cataclysmic email hacks that have afflicted everyone from Sony to John Podesta, and millions of ordinary consumers might be spared routinized identity theft. If Tim Berners-Lee, the inventor of the World Wide Web, had included a protocol for mapping our social identity in his original specs, we might not have Facebook.

The true believers behind blockchain platforms like Ethereum argue that a network of distributed trust is one of those advances in software architecture that will prove, in the long run, to have historic significance. That promise has helped fuel the huge jump in cryptocurrency valuations. But in a way, the Bitcoin bubble may ultimately turn out to be a distraction from the true significance of the blockchain. The real promise of these new technologies, many of their evangelists believe, lies not in displacing our currencies but in replacing much of what we now think of as the internet, while at the same time returning the online world to a more

decentralized and egalitarian system. If you believe the evangelists, the blockchain is the future. But it is also a way of getting back to the internet's roots.

Once the inspiration for utopian dreams of infinite libraries and global connectivity, the internet has seemingly become, over the past year, a universal scapegoat: the cause of almost every social ill that confronts us. Russian trolls destroy the democratic system with fake news on Facebook; hate speech flourishes on Twitter and Reddit; the vast fortunes of the geek elite worsen income equality. For many of us who participated in the early days of the web, the last few years have felt almost postlapsarian. The web had promised a new kind of egalitarian media, populated by small magazines, bloggers and self-organizing encyclopedias; the information titans that dominated mass culture in the 20th century would give way to a more decentralized system, defined by collaborative networks, not hierarchies and broadcast channels. The wider culture would come to mirror the peer-to-peer architecture of the internet itself. The web in those days was hardly a utopia — there were financial bubbles and spammers and a thousand other problems — but beneath those flaws, we assumed, there was an underlying story of progress.

Last year marked the point at which that narrative finally collapsed. The existence of internet skeptics is nothing new, of course; the difference now is that the critical voices increasingly belong to former enthusiasts. "We have to fix the internet," Walter Isaacson, Steve Jobs's biographer, wrote in an essay published a few weeks after Donald Trump was elected president. "After 40 years, it has begun to corrode, both itself and us." The former Google strategist James Williams told The Guardian: "The dynamics of the attention economy are structurally set up to undermine the human will." In a blog post, Brad Burnham, a managing partner at Union Square Ventures, a top New York venture-capital firm, bemoaned the collateral damage from the quasi monopolies of the digital age: "Publishers find themselves becoming commodity content suppliers in a sea of undifferentiated content in the Facebook news feed. Websites see their fortunes upended by small changes in Google's search algorithms. And manufacturers watch helplessly as sales dwindle when Amazon decides to source products directly in China and redirect demand to their own products." (Full disclosure: Burnham's firm invested in a company I started in 2006; we have had no financial relationship since it sold in 2011.) Even Berners-Lee, the inventor of the web itself, wrote a blog post voicing his

concerns that the advertising-based model of social media and search engines creates a climate where "misinformation, or 'fake news,' which is surprising, shocking or designed to appeal to our biases, can spread like wildfire."

For most critics, the solution to these immense structural issues has been to propose either a new mindfulness about the dangers of these tools — turning off our smartphones, keeping kids off social media — or the strong arm of regulation and antitrust: making the tech giants subject to the same scrutiny as other industries that are vital to the public interest, like the railroads or telephone networks of an earlier age. Both those ideas are commendable: We probably should develop a new set of habits governing how we interact with social media, and it seems entirely sensible that companies as powerful as Google and Facebook should face the same regulatory scrutiny as, say, television networks. But those interventions are unlikely to fix the core problems that the online world confronts. After all, it was not just the antitrust division of the Department of Justice that challenged Microsoft's monopoly power in the 1990s; it was also the emergence of new software and hardware — the web, open-source software and Apple products — that helped undermine Microsoft's dominant position.

The blockchain evangelists behind platforms like Ethereum believe that a comparable array of advances in software, cryptography and distributed systems has the ability to tackle today's digital problems: the corrosive incentives of online advertising; the quasi monopolies of Facebook, Google and Amazon; Russian misinformation campaigns. If they succeed, their creations may challenge the hegemony of the tech giants far more effectively than any antitrust regulation. They even claim to offer an alternative to the winner-take-all model of capitalism than has driven wealth inequality to heights not seen since the age of the robber barons.

That remedy is not yet visible in any product that would be intelligible to an ordinary tech consumer. The only blockchain project that has crossed over into mainstream recognition so far is Bitcoin, which is in the middle of a speculative bubble that makes the 1990s internet I.P.O. frenzy look like a neighborhood garage sale. And herein lies the cognitive dissonance that confronts anyone trying to make sense of the blockchain: the potential power of this would-be revolution is being actively undercut by the crowd it is attracting, a veritable goon squad of charlatans,

false prophets and mercenaries. Not for the first time, technologists pursuing a vision of an open and decentralized network have found themselves surrounded by a wave of opportunists looking to make an overnight fortune. The question is whether, after the bubble has burst, the very real promise of the blockchain can endure.

To some students of modern technological history, the internet's fall from grace follows an inevitable historical script. As Tim Wu argued in his 2010 book, "The Master Switch," all the major information technologies of the 20th century adhered to a similar developmental pattern, starting out as the playthings of hobbyists and researchers motivated by curiosity and community, and ending up in the hands of multinational corporations fixated on maximizing shareholder value. Wu calls this pattern the Cycle, and on the surface at least, the internet has followed the Cycle with convincing fidelity. The internet began as a hodgepodge of government-funded academic research projects and side-hustle hobbies. But 20 years after the web first crested into the popular imagination, it has produced in Google, Facebook and Amazon — and indirectly, Apple — what may well be the most powerful and valuable corporations in the history of capitalism.

Blockchain advocates don't accept the inevitability of the Cycle. The roots of the internet were in fact more radically open and decentralized than previous information technologies, they argue, and had we managed to stay true to those roots, it could have remained that way. The online world would not be dominated by a handful of information-age titans; our news platforms would be less vulnerable to manipulation and fraud; identity theft would be far less common; advertising dollars would be distributed across a wider range of media properties.

To understand why, it helps to think of the internet as two fundamentally different kinds of systems stacked on top of each other, like layers in an archaeological dig. One layer is composed of the software protocols that were developed in the 1970s and 1980s and hit critical mass, at least in terms of audience, in the 1990s. (A protocol is the software version of a lingua franca, a way that multiple computers agree to communicate with one another. There are protocols that govern the flow of the internet's raw data, and protocols for sending email messages, and protocols that define the addresses of web pages.) And then above

them, a second layer of web-based services — Facebook, Google, Amazon, Twitter — that largely came to power in the following decade.

The first layer — call it InternetOne — was founded on open protocols, which in turn were defined and maintained by academic researchers and international-standards bodies, owned by no one. In fact, that original openness continues to be all around us, in ways we probably don't appreciate enough. Email is still based on the open protocols POP, SMTP and IMAP; websites are still served up using the open protocol HTTP; bits are still circulated via the original open protocols of the internet, TCP/IP. You don't need to understand anything about how these software conventions work on a technical level to enjoy their benefits. The key characteristic they all share is that anyone can use them, free of charge. You don't need to pay a licensing fee to some corporation that owns HTTP if you want to put up a web page; you don't have to sell a part of your identity to advertisers if you want to send an email using SMTP. Along with Wikipedia, the open protocols of the internet constitute the most impressive example of commons-based production in human history.

To see how enormous but also invisible the benefits of such protocols have been, imagine that one of those key standards had not been developed: for instance, the open standard we use for defining our geographic location, GPS. Originally developed by the United States military, the Global Positioning System was first made available for civilian use during the Reagan administration. For about a decade, it was largely used by the aviation industry, until individual consumers began to use it in car navigation systems. And now we have smartphones that can pick up a signal from GPS satellites orbiting above us, and we use that extraordinary power to do everything from locating nearby restaurants to playing Pokémon Go to coordinating disaster-relief efforts.

But what if the military had kept GPS out of the public domain? Presumably, sometime in the 1990s, a market signal would have gone out to the innovators of Silicon Valley and other tech hubs, suggesting that consumers were interested in establishing their exact geographic coordinates so that those locations could be projected onto digital maps. There would have been a few years of furious competition among rival companies, who would toss their own proprietary satellites

into orbit and advance their own unique protocols, but eventually the market would have settled on one dominant model, given all the efficiencies that result from a single, common way of verifying location. Call that imaginary firm GeoBook. Initially, the embrace of GeoBook would have been a leap forward for consumers and other companies trying to build location awareness into their hardware and software. But slowly, a darker narrative would have emerged: a single private corporation, tracking the movements of billions of people around the planet, building an advertising behemoth based on our shifting locations. Any start-up trying to build a geo-aware application would have been vulnerable to the whims of mighty GeoBook. Appropriately angry polemics would have been written denouncing the public menace of this Big Brother in the sky.

But none of that happened, for a simple reason. Geolocation, like the location of web pages and email addresses and domain names, is a problem we solved with an open protocol. And because it's a problem we don't have, we rarely think about how beautifully GPS does work and how many different applications have been built on its foundation.

The open, decentralized web turns out to be alive and well on the InternetOne layer. But since we settled on the World Wide Web in the mid-'90s, we've adopted very few new open-standard protocols. The biggest problems that technologists tackled after 1995 — many of which revolved around identity, community and payment mechanisms — were left to the private sector to solve. This is what led, in the early 2000s, to a powerful new layer of internet services, which we might call InternetTwo.

For all their brilliance, the inventors of the open protocols that shaped the internet failed to include some key elements that would later prove critical to the future of online culture. Perhaps most important, they did not create a secure open standard that established human identity on the network. Units of information could be defined — pages, links, messages — but *people* did not have their own protocol: no way to define and share your real name, your location, your interests or (perhaps most crucial) your relationships to other people online.

This turns out to have been a major oversight, because identity is the sort of problem that benefits from one universally recognized solution. It's what Vitalik Buterin, a founder of Ethereum, describes as "base-layer" infrastructure: things like language, roads and postal services, platforms where commerce and competition are actually assisted by having an underlying layer in the public domain. Offline, we don't have an open market for physical passports or Social Security numbers; we have a few reputable authorities — most of them backed by the power of the state — that we use to confirm to others that we are who we say we are. But online, the private sector swooped in to fill that vacuum, and because identity had that characteristic of being a universal problem, the market was heavily incentivized to settle on one common standard for defining yourself and the people you know.

The self-reinforcing feedback loops that economists call "increasing returns" or "network effects" kicked in, and after a period of experimentation in which we dabbled in social-media start-ups like Myspace and Friendster, the market settled on what is essentially a proprietary standard for establishing who you are and whom you know. That standard is Facebook. With more than two billion users, Facebook is far larger than the entire internet at the peak of the dot-com bubble in the late 1990s. And that user growth has made it the world's sixth-most-valuable corporation, just 14 years after it was founded. Facebook is the ultimate embodiment of the chasm that divides InternetOne and InternetTwo economies. No private company owned the protocols that defined email or GPS or the open web. But one single corporation owns the data that define social identity for two billion people today — and one single person, Mark Zuckerberg, holds the majority of the voting power in that corporation.

If you see the rise of the centralized web as an inevitable turn of the Cycle, and the open-protocol idealism of the early web as a kind of adolescent false consciousness, then there's less reason to fret about all the ways we've abandoned the vision of InternetOne. Either we're living in a fallen state today and there's no way to get back to Eden, or Eden itself was a kind of fantasy that was always going to be corrupted by concentrated power. In either case, there's no point in trying to restore the architecture of InternetOne; our only hope is to use the power of the state to rein in these corporate giants, through regulation and antitrust action. It's a variation of the old Audre Lorde maxim: "The master's tools will never dismantle the

master's house." You can't fix the problems technology has created for us by throwing more technological solutions at it. You need forces outside the domain of software and servers to break up cartels with this much power.

But the thing about the master's house, in this analogy, is that it's a duplex. The upper floor has indeed been built with tools that cannot be used to dismantle it. But the open protocols beneath them still have the potential to build something better.

One of the most persuasive advocates of an open-protocol revival is Juan Benet, a Mexican-born programmer now living on a suburban side street in Palo Alto, Calif., in a three-bedroom rental that he shares with his girlfriend and another programmer, plus a rotating cast of guests, some of whom belong to Benet's organization, Protocol Labs. On a warm day in September, Benet greeted me at his door wearing a black Protocol Labs hoodie. The interior of the space brought to mind the incubator/frat house of HBO's "Silicon Valley," its living room commandeered by an array of black computer monitors. In the entrance hallway, the words "Welcome to Rivendell" were scrawled out on a whiteboard, a nod to the Elven city from "Lord of the Rings." "We call this house Rivendell," Benet said sheepishly. "It's not a very good Rivendell. It doesn't have enough books, or waterfalls, or elves."

Benet, who is 29, considers himself a child of the first peer-to-peer revolution that briefly flourished in the late 1990s and early 2000s, driven in large part by networks like BitTorrent that distributed media files, often illegally. That initial flowering was in many ways a logical outgrowth of the internet's decentralized, open-protocol roots. The web had shown that you could publish documents reliably in a commons-based network. Services like BitTorrent or Skype took that logic to the next level, allowing ordinary users to add new functionality to the internet: creating a distributed library of (largely pirated) media, as with BitTorrent, or helping people make phone calls over the internet, as with Skype.

Sitting in the living room/office at Rivendell, Benet told me that he thinks of the early 2000s, with the ascent of Skype and BitTorrent, as "the 'summer' of peer-to-peer" — its salad days. "But then peer-to-peer hit a wall, because people started to prefer centralized architectures," he said. "And partly because the peer-to-peer business models were piracy-driven." A graduate of Stanford's computer-science

program, Benet talks in a manner reminiscent of Elon Musk: As he speaks, his eyes dart across an empty space above your head, almost as though he's reading an invisible teleprompter to find the words. He is passionate about the technology Protocol Labs is developing, but also keen to put it in a wider context. For Benet, the shift from distributed systems to more centralized approaches set in motion changes that few could have predicted. "The rules of the game, the rules that govern all of this technology, matter a lot," he said. "The structure of what we build now will paint a very different picture of the way things will be five or 10 years in the future." He continued: "It was clear to me then that peer-to-peer was this extraordinary thing. What was not clear to me then was how at risk it is. It was not clear to me that you had to take up the baton, that it's now your turn to protect it."

Protocol Labs is Benet's attempt to take up that baton, and its first project is a radical overhaul of the internet's file system, including the basic scheme we use to address the location of pages on the web. Benet calls his system IPFS, short for InterPlanetary File System. The current protocol — HTTP — pulls down web pages from a single location at a time and has no built-in mechanism for archiving the online pages. IPFS allows users to download a page simultaneously from multiple locations and includes what programmers call "historic versioning," so that past iterations do not vanish from the historical record. To support the protocol, Benet is also creating a system called Filecoin that will allow users to effectively rent out unused hard-drive space. (Think of it as a sort of Airbnb for data.) "Right now there are tons of hard drives around the planet that are doing nothing, or close to nothing, to the point where their owners are just losing money," Benet said. "So you can bring online a massive amount of supply, which will bring down the costs of storage." But as its name suggests, Protocol Labs has an ambition that extends beyond these projects; Benet's larger mission is to support many new open-source protocols in the years to come.

Why did the internet follow the path from open to closed? One part of the explanation lies in sins of omission: By the time a new generation of coders began to tackle the problems that InternetOne left unsolved, there were near-limitless sources of capital to invest in those efforts, so long as the coders kept their systems closed. The secret to the success of the open protocols of InternetOne is that they were developed in an age when most people didn't care about online networks, so they

were able to stealthily reach critical mass without having to contend with wealthy conglomerates and venture capitalists. By the mid-2000s, though, a promising new start-up like Facebook could attract millions of dollars in financing even before it became a household brand. And that private-sector money ensured that the company's key software would remain closed, in order to capture as much value as possible for shareholders.

And yet — as the venture capitalist Chris Dixon points out — there was another factor, too, one that was more technical than financial in nature. "Let's say you're trying to build an open Twitter," Dixon explained while sitting in a conference room at the New York offices of Andreessen Horowitz, where he is a general partner. "I'm @cdixon at Twitter. Where do you store that? You need a database." A closed architecture like Facebook's or Twitter's puts all the information about its users — their handles, their likes and photos, the map of connections they have to other individuals on the network — into a private database that is maintained by the company. Whenever you look at your Facebook newsfeed, you are granted access to some infinitesimally small section of that database, seeing only the information that is relevant to you.

Running Facebook's database is an unimaginably complex operation, relying on hundreds of thousands of servers scattered around the world, overseen by some of the most brilliant engineers on the planet. From Facebook's point of view, they're providing a valuable service to humanity: creating a common social graph for almost everyone on earth. The fact that they have to sell ads to pay the bills for that service — and the fact that the scale of their network gives them staggering power over the minds of two billion people around the world — is an unfortunate, but inevitable, price to pay for a shared social graph. And that trade-off did in fact make sense in the mid-2000s; creating a single database capable of tracking the interactions of hundreds of millions of people — much less two billion — was the kind of problem that could be tackled only by a single organization. But as Benet and his fellow blockchain evangelists are eager to prove, that might not be true anymore.

So how can you get meaningful adoption of base-layer protocols in an age when the big tech companies have already attracted billions of users and collectively sit on hundreds of billions of dollars in cash? If you happen to believe that the internet, in

its current incarnation, is causing significant and growing harm to society, then this seemingly esoteric problem — the difficulty of getting people to adopt new open-source technology standards — turns out to have momentous consequences. If we can't figure out a way to introduce new, rival base-layer infrastructure, then we're stuck with the internet we have today. The best we can hope for is government interventions to scale back the power of Facebook or Google, or some kind of consumer revolt that encourages that marketplace to shift to less hegemonic online services, the digital equivalent of forswearing big agriculture for local farmers' markets. Neither approach would upend the underlying dynamics of InternetTwo.

The first hint of a meaningful challenge to the closed-protocol era arrived in 2008, not long after Zuckerberg opened the first international headquarters for his growing company. A mysterious programmer (or group of programmers) going by the name Satoshi Nakamoto circulated a paper on a cryptography mailing list. The paper was called "Bitcoin: A Peer-to-Peer Electronic Cash System," and in it, Nakamoto outlined an ingenious system for a digital currency that did not require a centralized trusted authority to verify transactions. At the time, Facebook and Bitcoin seemed to belong to entirely different spheres — one was a booming venture-backed social-media start-up that let you share birthday greetings and connect with old friends, while the other was a byzantine scheme for cryptographic currency from an obscure email list. But 10 years later, the ideas that Nakamoto unleashed with that paper now pose the most significant challenge to the hegemony of InternetTwo giants like Facebook.

The paradox about Bitcoin is that it may well turn out to be a genuinely revolutionary breakthrough and at the same time a colossal failure as a currency. As I write, Bitcoin has increased in value by nearly 100,000 percent over the past five years, making a fortune for its early investors but also branding it as a spectacularly unstable payment mechanism. The process for creating new Bitcoins has also turned out to be a staggering energy drain.

History is replete with stories of new technologies whose initial applications end up having little to do with their eventual use. All the focus on Bitcoin as a payment system may similarly prove to be a distraction, a technological red herring. Nakamoto pitched Bitcoin as a "peer-to-peer electronic-cash system" in the initial

manifesto, but at its heart, the innovation he (or she or they) was proposing had a more general structure, with two key features.

First, Bitcoin offered a kind of proof that you could create a secure database — the blockchain — scattered across hundreds or thousands of computers, with no single authority controlling and verifying the authenticity of the data.

Second, Nakamoto designed Bitcoin so that the work of maintaining that distributed ledger was itself rewarded with small, increasingly scarce Bitcoin payments. If you dedicated half your computer's processing cycles to helping the Bitcoin network get its math right — and thus fend off the hackers and scam artists — you received a small sliver of the currency. Nakamoto designed the system so that Bitcoins would grow increasingly difficult to earn over time, ensuring a certain amount of scarcity in the system. If you helped Bitcoin keep that database secure in the early days, you would earn more Bitcoin than later arrivals. This process has come to be called "mining."

For our purposes, forget everything else about the Bitcoin frenzy, and just keep these two things in mind: What Nakamoto ushered into the world was a way of agreeing on the contents of a database without anyone being "in charge" of the database, and a way of compensating people for helping make that database more valuable, without those people being on an official payroll or owning shares in a corporate entity. Together, those two ideas solved the distributed-database problem and the funding problem. Suddenly there was a way of supporting open protocols that wasn't available during the infancy of Facebook and Twitter.

These two features have now been replicated in dozens of new systems inspired by Bitcoin. One of those systems is Ethereum, proposed in a white paper by Vitalik Buterin when he was just 19. Ethereum does have its currencies, but at its heart Ethereum was designed less to facilitate electronic payments than to allow people to run applications on top of the Ethereum blockchain. There are currently hundreds of Ethereum apps in development, ranging from prediction markets to Facebook clones to crowdfunding services. Almost all of them are in pre-alpha stage, not ready for consumer adoption. Despite the embryonic state of the applications, the Ether

currency has seen its own miniature version of the Bitcoin bubble, most likely making Buterin an immense fortune.

These currencies can be used in clever ways. Juan Benet's Filecoin system will rely on Ethereum technology and reward users and developers who adopt its IPFS protocol or help maintain the shared database it requires. Protocol Labs is creating its own cryptocurrency, also called Filecoin, and has plans to sell some of those coins on the open market in the coming months. (In the summer of 2017, the company raised $135 million in the first 60 minutes of what Benet calls a "presale" of the tokens to accredited investors.) Many cryptocurrencies are first made available to the public through a process known as an initial coin offering, or I.C.O.

The I.C.O. abbreviation is a deliberate echo of the initial public offering that so defined the first internet bubble in the 1990s. But there is a crucial difference between the two. Speculators can buy in during an I.C.O., but they are not buying an ownership stake in a private company and its proprietary software, the way they might in a traditional I.P.O. Afterward, the coins will continue to be created in exchange for labor — in the case of Filecoin, by anyone who helps maintain the Filecoin network. Developers who help refine the software can earn the coins, as can ordinary users who lend out spare hard-drive space to expand the network's storage capacity. The Filecoin is a way of signaling that someone, somewhere, has added value to the network.

Advocates like Chris Dixon have started referring to the compensation side of the equation in terms of "tokens," not coins, to emphasize that the technology here isn't necessarily aiming to disrupt existing currency systems. "I like the metaphor of a token because it makes it very clear that it's like an arcade," he says. "You go to the arcade, and in the arcade you can use these tokens. But we're not trying to replace the U.S. government. It's not meant to be a real currency; it's meant to be a pseudo-currency inside this world." Dan Finlay, a creator of MetaMask, echoes Dixon's argument. "To me, what's interesting about this is that we get to program new value systems," he says. "They don't have to resemble money."

Pseudo or not, the idea of an I.C.O. has already inspired a host of shady offerings, some of them endorsed by celebrities who would seem to be unlikely

blockchain enthusiasts, like DJ Khaled, Paris Hilton and Floyd Mayweather. In a blog post published in October 2017, Fred Wilson, a founder of Union Square Ventures and an early advocate of the blockchain revolution, thundered against the spread of I.C.O.s. “I hate it,” Wilson wrote, adding that most I.C.O.s “are scams. And the celebrities and others who promote them on their social-media channels in an effort to enrich themselves are behaving badly and possibly violating securities laws.” Arguably the most striking thing about the surge of interest in I.C.O.s — and in existing currencies like Bitcoin or Ether — is how much financial speculation has already gravitated to platforms that have effectively zero adoption among ordinary consumers. At least during the internet bubble of late 1990s, ordinary people were buying books on Amazon or reading newspapers online; there was clear evidence that the web was going to become a mainstream platform. Today, the hype cycles are so accelerated that billions of dollars are chasing a technology that almost no one outside the cryptocommunity understands, much less uses.

Let’s say, for the sake of argument, that the hype is warranted, and blockchain platforms like Ethereum become a fundamental part of our digital infrastructure. How would a distributed ledger and a token economy somehow challenge one of the tech giants? One of Fred Wilson’s partners at Union Square Ventures, Brad Burnham, suggests a scenario revolving around another tech giant that has run afoul of regulators and public opinion in the last year: Uber. “Uber is basically just a coordination platform between drivers and passengers,” Burnham says. “Yes, it was really innovative, and there were a bunch of things in the beginning about reducing the anxiety of whether the driver was coming or not, and the map — and a whole bunch of things that you should give them a lot of credit for.” But when a new service like Uber starts to take off, there’s a strong incentive for the marketplace to consolidate around a single leader. The fact that more passengers are starting to use the Uber app attracts more drivers to the service, which in turn attracts more passengers. People have their credit cards stored with Uber; they have the app installed already; there are far more Uber drivers on the road. And so the switching costs of trying out some other rival service eventually become prohibitive, even if the chief executive seems to be a jerk or if consumers would, in the abstract, prefer a competitive marketplace with a dozen Ubers. “At some point, the innovation around the coordination becomes less and less innovative,” Burnham says.

The blockchain world proposes something different. Imagine some group like Protocol Labs decides there's a case to be made for adding another "basic layer" to the stack. Just as GPS gave us a way of discovering and sharing our location, this new protocol would define a simple request: I am here and would like to go there. A distributed ledger might record all its users' past trips, credit cards, favorite locations — all the metadata that services like Uber or Amazon use to encourage lock-in. Call it, for the sake of argument, the Transit protocol. The standards for sending a Transit request out onto the internet would be entirely open; anyone who wanted to build an app to respond to that request would be free to do so. Cities could build Transit apps that allowed taxi drivers to field requests. But so could bike-share collectives, or rickshaw drivers. Developers could create shared marketplace apps where all the potential vehicles using Transit could vie for your business. When you walked out on the sidewalk and tried to get a ride, you wouldn't have to place your allegiance with a single provider before hailing. You would simply announce that you were standing at 67th and Madison and needed to get to Union Square. And then you'd get a flurry of competing offers. You could even theoretically get an offer from the M.T.A., which could build a service to remind Transit users that it might be much cheaper and faster just to jump on the 6 train.

How would Transit reach critical mass when Uber and Lyft already dominate the ride-sharing market? This is where the tokens come in. Early adopters of Transit would be rewarded with Transit tokens, which could themselves be used to purchase Transit services or be traded on exchanges for traditional currency. As in the Bitcoin model, tokens would be doled out less generously as Transit grew more popular. In the early days, a developer who built an iPhone app that uses Transit might see a windfall of tokens; Uber drivers who started using Transit as a second option for finding passengers could collect tokens as a reward for embracing the system; adventurous consumers would be rewarded with tokens for using Transit in its early days, when there are fewer drivers available compared with the existing proprietary networks like Uber or Lyft.

As Transit began to take off, it would attract speculators, who would put a monetary price on the token and drive even more interest in the protocol by inflating its value, which in turn would attract more developers, drivers and customers. If the whole system ends up working as its advocates believe, the result is a more

competitive but at the same time more equitable marketplace. Instead of all the economic value being captured by the shareholders of one or two large corporations that dominate the market, the economic value is distributed across a much wider group: the early developers of Transit, the app creators who make the protocol work in a consumer-friendly form, the early-adopter drivers and passengers, the first wave of speculators. Token economies introduce a strange new set of elements that do not fit the traditional models: instead of creating value by owning something, as in the shareholder equity model, people create value by improving the underlying protocol, either by helping to maintain the ledger (as in Bitcoin mining), or by writing apps atop it, or simply by using the service. The lines between founders, investors and customers are far blurrier than in traditional corporate models; all the incentives are explicitly designed to steer away from winner-take-all outcomes. And yet at the same time, the whole system depends on an initial speculative phase in which outsiders are betting on the token to rise in value.

"You think about the '90s internet bubble and all the great infrastructure we got out of that," Dixon says. "You're basically taking that effect and shrinking it down to the size of an application."

Even decentralized cryptomovements have their key nodes. For Ethereum, one of those nodes is the Brooklyn headquarters of an organization called ConsenSys, founded by Joseph Lubin, an early Ethereum pioneer. In November, Amanda Gutterman, the 26-year-old chief marketing officer for ConsenSys, gave me a tour of the space. In our first few minutes together, she offered the obligatory cup of coffee, only to discover that the drip-coffee machine in the kitchen was bone dry. "How can we fix the internet if we can't even make coffee?" she said with a laugh.

Planted in industrial Bushwick, a stone's throw from the pizza mecca Roberta's, "headquarters" seemed an unlikely word. The front door was festooned with graffiti and stickers; inside, the stairwells of the space appeared to have been last renovated during the Coolidge administration. Just about three years old, the ConsenSys network now includes more than 550 employees in 28 countries, and the operation has never raised a dime of venture capital. As an organization, ConsenSys does not quite fit any of the usual categories: It is technically a corporation, but it has elements that also resemble nonprofits and workers' collectives. The shared goal of

ConsenSys members is strengthening and expanding the Ethereum blockchain. They support developers creating new apps and tools for the platform, one of which is MetaMask, the software that generated my Ethereum address. But they also offer consulting-style services for companies, nonprofits or governments looking for ways to integrate Ethereum's smart contracts into their own systems.

The true test of the blockchain will revolve — like so many of the online crises of the past few years — around the problem of identity. Today your digital identity is scattered across dozens, or even hundreds, of different sites: Amazon has your credit-card information and your purchase history; Facebook knows your friends and family; Equifax maintains your credit history. When you use any of those services, you are effectively asking for permission to borrow some of that information about yourself in order perform a task: ordering a Christmas present for your uncle, checking Instagram to see pictures from the office party last night. But all these different fragments of your identity don't belong to you; they belong to Facebook and Amazon and Google, who are free to sell bits of that information about you to advertisers without consulting you. You, of course, are free to delete those accounts if you choose, and if you stop checking Facebook, Zuckerberg and the Facebook shareholders will stop making money by renting out your attention to their true customers. But your Facebook or Google identity isn't portable. If you want to join another promising social network that is maybe a little less infected with Russian bots, you can't extract your social network from Twitter and deposit it in the new service. You have to build the network again from scratch (and persuade all your friends to do the same).

The blockchain evangelists think this entire approach is backward. You should own your digital identity — which could include everything from your date of birth to your friend networks to your purchasing history — and you should be free to lend parts of that identity out to services as you see fit. Given that identity was not baked into the original internet protocols, and given the difficulty of managing a distributed database in the days before Bitcoin, this form of "self-sovereign" identity — as the parlance has it — was a practical impossibility. Now it is an attainable goal. A number of blockchain-based services are trying to tackle this problem, including a new identity system called uPort that has been spun out of ConsenSys and another one called Blockstack that is currently based on the Bitcoin platform. (Tim Berners-

Lee is leading the development of a comparable system, called Solid, that would also give users control over their own data.) These rival protocols all have slightly different frameworks, but they all share a general vision of how identity should work on a truly decentralized internet.

What would prevent a new blockchain-based identity standard from following Tim Wu's Cycle, the same one that brought Facebook to such a dominant position? Perhaps nothing. But imagine how that sequence would play out in practice. Someone creates a new protocol to define your social network via Ethereum. It might be as simple as a list of other Ethereum addresses; in other words, *Here are the public addresses of people I like and trust*. That way of defining your social network might well take off and ultimately supplant the closed systems that define your network on Facebook. Perhaps someday, every single person on the planet might use that standard to map their social connections, just as every single person on the internet uses TCP/IP to share data. But even if this new form of identity became ubiquitous, it wouldn't present the same opportunities for abuse and manipulation that you find in the closed systems that have become de facto standards. I might allow a Facebook-style service to use my social map to filter news or gossip or music for me, based on the activity of my friends, but if that service annoyed me, I'd be free to sample other alternatives without the switching costs. An open identity standard would give ordinary people the opportunity to sell their attention to the highest bidder, or choose to keep it out of the marketplace altogether.

Gutterman suggests that the same kind of system could be applied to even more critical forms of identity, like health care data. Instead of storing, say, your genome on servers belonging to a private corporation, the information would instead be stored inside a personal data archive. "There may be many corporate entities that I don't want seeing that data, but maybe I'd like to donate that data to a medical study," she says. "I could use my blockchain-based self-sovereign ID to [allow] one group to use it and not another. Or I could sell it over here and give it away over there."

The token architecture would give a blockchain-based identity standard an additional edge over closed standards like Facebook's. As many critics have observed, ordinary users on social-media platforms create almost all the content

without compensation, while the companies capture all the economic value from that content through advertising sales. A token-based social network would at least give early adopters a piece of the action, rewarding them for their labors in making the new platform appealing. “If someone can really figure out a version of Facebook that lets users own a piece of the network and get paid,” Dixon says, “that could be pretty compelling.”

Would that information be more secure in a distributed blockchain than behind the elaborate firewalls of giant corporations like Google or Facebook? In this one respect, the Bitcoin story is actually instructive: It may never be stable enough to function as a currency, but it does offer convincing proof of just how secure a distributed ledger can be. “Look at the market cap of Bitcoin or Ethereum: $80 billion, $25 billion, whatever,” Dixon says. “That means if you successfully attack that system, you could walk away with more than a billion dollars. You know what a ‘bug bounty’ is? Someone says, ‘If you hack my system, I’ll give you a million dollars.’ So Bitcoin is now a nine-year-old multibillion-dollar bug bounty, and no one’s hacked it. It feels like pretty good proof.”

Additional security would come from the decentralized nature of these new identity protocols. In the identity system proposed by Blockstack, the actual information about your identity — your social connections, your purchasing history — could be stored anywhere online. The blockchain would simply provide cryptographically secure keys to unlock that information and share it with other trusted providers. A system with a centralized repository with data for hundreds of millions of users — what security experts call “honey pots” — is far more appealing to hackers. Which would you rather do: steal a hundred million credit histories by hacking into a hundred million separate personal computers and sniffing around until you found the right data on each machine? Or just hack into one honey pot at Equifax and walk away with the same amount of data in a matter of hours? As Gutterman puts it, “It’s the difference between robbing a house versus robbing the entire village.”

So much of the blockchain’s architecture is shaped by predictions about how that architecture might be abused once it finds a wider audience. That is part of its charm and its power. The blockchain channels the energy of speculative bubbles by

allowing tokens to be shared widely among true supporters of the platform. It safeguards against any individual or small group gaining control of the entire database. Its cryptography is designed to protect against surveillance states or identity thieves. In this, the blockchain displays a familial resemblance to political constitutions: Its rules are designed with one eye on how those rules might be exploited down the line.

Much has been made of the anarcho-libertarian streak in Bitcoin and other nonfiat currencies; the community is rife with words and phrases ("self-sovereign") that sound as if they could be slogans for some militia compound in Montana. And yet in its potential to break up large concentrations of power and explore less-proprietary models of ownership, the blockchain idea offers a tantalizing possibility for those who would like to distribute wealth more equitably and break up the cartels of the digital age.

The blockchain worldview can also sound libertarian in the sense that it proposes nonstate solutions to capitalist excesses like information monopolies. But to believe in the blockchain is not necessarily to oppose regulation, if that regulation is designed with complementary aims. Brad Burnham, for instance, suggests that regulators should insist that everyone have "a right to a private data store," where all the various facets of their online identity would be maintained. But governments wouldn't be required to design those identity protocols. They would be developed on the blockchain, open source. Ideologically speaking, that private data store would be a true team effort: built as an intellectual commons, funded by token speculators, supported by the regulatory state.

Like the original internet itself, the blockchain is an idea with radical — almost communitarian — possibilities that at the same time has attracted some of the most frivolous and regressive appetites of capitalism. We spent our first years online in a world defined by open protocols and intellectual commons; we spent the second phase in a world increasingly dominated by closed architectures and proprietary databases. We have learned enough from this history to support the hypothesis that open works better than closed, at least where base-layer issues are concerned. But we don't have an easy route back to the open-protocol era. Some messianic next-

generation internet protocol is not likely to emerge out of Department of Defense research, the way the first-generation internet did nearly 50 years ago.

Yes, the blockchain may seem like the very worst of speculative capitalism right now, and yes, it is demonically challenging to understand. But the beautiful thing about open protocols is that they can be steered in surprising new directions by the people who discover and champion them in their infancy. Right now, the only real hope for a revival of the open-protocol ethos lies in the blockchain. Whether it eventually lives up to its egalitarian promise will in large part depend on the people who embrace the platform, who take up the baton, as Juan Benet puts it, from those early online pioneers. If you think the internet is not working in its current incarnation, you can't change the system through think-pieces and F.C.C. regulations alone. You need new code.

Steven Johnson is the author of 10 books, most recently "Wonderland." He last wrote for the magazine about the science of communicating with extraterrestrials.

Sign up for our newsletter to get the best of The New York Times Magazine delivered to your inbox every week.

A version of this article appears in print on January 21, 2018, on Page MM36 of the Sunday Magazine with the headline: Beyond the Bitcoin Bubble.
