FEVER

Cryptographic sorcery, entrepreneurial zeal, and utopian dreams have gripped a striking number of Penn students and alumni this year. Why are people so excited?

By Trey Popp

When he moved off campus as a junior, Dillon Chen W'18 faced a situation that irks every city dweller rankled by the price of residential internet access. His laptop registered 15 wireless signals—representing more bandwidth than he'd ever need—but every one was locked. Wouldn't it be great, he thought, if there were a secure way to incentivize people to share their signals with strangers? Then he thought some more, and landed on a new tool that seemed purpose-made to pull off that trick.

Around the same time, Diego Espinosa WG'91, a longtime equities analyst and investor who has also taught finance at the University of San Diego School of Business, had an epiphany about how to turn diabetes prevention into a business venture. Betting on the same technology that interested Dillon Chen, he hit the off-ramp from traditional capital markets and bee-lined toward a sector people were beginning to call the Next Internet. Halfway around the world, Mir Haque WG'08 soon found himself pitching the same tech platform to government officials in his native Bangladesh—as a way to extend financial services to unbanked citizens and refugees. Meanwhile, back on campus, a molecular biologist named Harvey Rubin Gr'74 was wrestling with a predicament of his own. He had piloted a program to supply remote areas of Zimbabwe with vaccines, which require continuous cold storage, by using cellphone towers to power refrigerators. It had helped inoculate 250,000 people. That had sparked interest in expanding to other countries, but it remained very difficult to guarantee the authenticity and storage conditions of the complex supply chain. Now Rubin had his own eureka moment: *This was a job for blockchain.*

Four very different problems, and four people convinced that the same tool held the solution. Not just a feasible solution, either, but one that seemed almost uncannily well-adapted to the challenge at hand. And when they took a step back, its potential seemed even more dramatic. Rubin soon saw it as a way to revolutionize financial transparency in the murky world of philanthropy. Haque envisioned taming the fraud-ridden chaos of local educational credentialing systems and merging them seamlessly with global labor markets, leveling a playing field long tilted against developing-world strivers. Espinosa glimpsed a chance for exploited subjects of social media empires to reclaim sovereignty over their own data—without having to wait for government intervention.

Blockchains are a novel type of database. They are most closely associated with Bitcoin, whose unknown creator invented the format as a foundation for a virtual currency. Bitcoin's tenfold price appreciation in 2017—along with the downright stupefying gains of other virtual coins, like Ethereum, whose value multiplied by a factor of 70—made the global cryptocurrency craze the story of the year. But that bubble may be the least important—and least interesting—thing about the technology underlying it.

ILLUSTRATION BY CHRIS GASH

Beneath a familiar surface, blockchain fever roiled Penn's campus this year with a mixture of entrepreneurial zeal, utopian fantasy, greed, confusion, naysaying, and intellectual electricity this reporter has only witnessed once before: in the San Francisco Bay Area during the original dot-com boom. Here was a group of students trying to put insurance on a blockchain. There was one developing a blockchain to enable gastroenterology practices to document endoscopies. Joshua Talbot WG'18 was working on a blockchain that home-healthcare agencies could use to certify patient interactions for Medicare/Medicaid reimbursement. Xiao Ling EAS'11 GEng'17 was part of a team building a cryptocurrency they hoped would accomplish nothing short of incentivizing "people to help each other more, and in the process communicate with each other in a more authentic manner."

Rarely do gold rushes spark such runaway idealism. "Blockchain as it helps business—like, *use this on our supply chain and it'll make things more efficient*, is definitely going to exist, and probably soon, in real capacities," I heard from Nate Rush, a College junior held in awe among campus tech types for his coding chops. But what really drove him was a headier prospect: "blockchain as it replaces business."

The Greeks had Plato's *Republic*. Revolutionary Germany begat Karl Marx. Industrial America gave rise to the Oneida religious perfectionists, the Shakers, and Robert Owen's experimental socialist cooperatives. Meanwhile, the great utopian hope of our era lies in … cryptographically based decentralized digital ledgers?

How has the emergence of blockchain ignited so many imaginations in so many different domains? Does it represent the final step in the digitalization of economic life? Will it do for assets what the internet did for information? Is it the death knell for "lawyers, brokers, and bankers," among the other white-collar middlemen *Harvard Business Review* put on notice last year?

Some enthusiasts envision blockchain transforming capitalism itself. Others see a scam of world-historical proportions. "This is not just a bubble," one prominent hedge fund advised clients in a January letter about cryptocurrencies. "It is not just a fraud. It is perhaps the outer limit, the ultimate expression, of the ability of humans to seize upon ether and hope to ride it to the stars." That's a lot of scorn to heap on one component of a tool that has attracted some of the 500-pound gorillas of global commerce: IBM, Walmart, Maersk, Google, Goldman Sachs, and so on. Even as cryptocurrency prices swooned in the first three months of 2018, venture capitalists invested half a billion dollars in 75 blockchain projects, according to the market-research company PitchBook.

David Crosbie is a lecturer in the School of Engineering and Applied Science who made his money creating companies that "built plumbing inside the Internet." He detected a familiar pattern in the inflamed rhetoric surrounding blockchain. "First you dismiss it as unimportant," he mused in February. "Then you embrace it. Then you try and kill it. And then you become it."

What might become of blockchain? Will it liberate the baby-picture-posting, *Like*-clicking, Waze-navigating masses from their data-snooping corporate overlords—or help 21st-century monopolists amass greater power still? Will it unleash the dormant market power of 2 billion unbanked adults around the world—or turn the digital divide into an apocalyptic abyss? Or are those patently absurd ways to think about a glorified ledger book?

In a search for answers—and a better sense of the right questions to ask—I audited a Wharton MBA class that focused partly on blockchain, taught this winter by visiting professor Shimon Kogan, who is based at Israel's Interdisciplinary Center Herzliya. I owe many insights to him. It is early days for blockchain, and academic offerings are scarce. Tom Baker, the William Maul Measey Professor of Law and Health Sciences, has also addressed blockchain as part of a broader seminar on tech-driven financial services, or FinTech. Next fall, Crosbie and Wharton associate professor Kevin Werbach will teach Penn's first full class on blockchain.

But in truth, University administrators are playing catch-up with students. The student-run Penn Blockchain Club, which has mushroomed to 400 members in the space of two years, has effectively mounted a miniature shadow college to satisfy the hunger for insights and technical know-how. Working with the Wharton Advisory Board to secure classroom space, its leaders have organized lectures by self-educated students—from code jockeys to cryptocurrency traders—and brought in speakers from organizations ranging from the Ethereum Foundation to the World Bank. So students were another source of insights, along with a number of alumni who are developers, investors, and aspiring thought-leaders in the blockchain realm.

It is a singularly strange place, where greed and gullibility rub up against technical sorcery in the fervid atmosphere of a Pentecostal tent revival. Speculation naturally outruns concrete achievements on any new technological frontier. But blockchains and cryptocurrencies, perhaps because they take some concerted effort to understand, have a way of utterly consuming the brains of people who've put in the work. "Welcome to the rabbit hole," I heard again and again from people who'd taken the plunge.

And there's no shortage of blue caterpillars down there, smoking hookahs atop mushroom caps.

But first there's a hall of locked doors, and opening them requires an acquaintance with a basic but far-reaching concept from cryptography.

The Hash: The Swiss Army Knife of Cryptography

A hash function is a mathematical algorithm with a simple basic purpose: It converts any string of numbers into another string of a standard length. The SHA-256 hash algorithm, for instance, converts any input into a 64-character string of numbers and letters (which actually represent two-digit integers). Since all digital data are represented numerically, any digital input can be hashed. The name "Jane Doe" produces a 64-character string. So does the last selfie you posted on Instagram. So does the unabridged text of *Moby-Dick*—and it will always produce the exact same hash. But—and here's the important thing—if even a single character of that text is altered, the resulting hash will be utterly unrecognizable from that of the unaltered text.

Take the title of this section. Its SHA-256 hash is a string that starts out like this: b03fec1465. But if we change *Knife* to *knife*, the hash diverges wildly, beginning: 983a7eb155.

That illuminates a key feature of hashes: they are one-way functions. Turning a given data packet into a hash is a matter of trivial computation, but it's impossible to reverse-engineer the process. If all you have is a hash, the only way to recreate the original data is by brute computational force: guessing every possible input until one produces a match.

Hashes have many uses. Reputable website operators do not store your passwords, for example, but rather hashes of them. (When you enter a password, it is hashed and compared against the stored hash; a match unlocks the door. In security breaches, what hackers actually obtain is a ledger of hashes. If they know which hash algorithm was used, they can apply it to guessed passwords in hopes of finding matches; that's why passwords like "12345" or "admin" or "password"—all hugely popular and therefore commonly guessed—are a bad idea.) Hashes are useful in indexing, since they turn giant data packets into tiny digital fingerprints that a computer can sift through much faster.

Hashes also form the cement that binds blockchains.

Satoshi's Bible

In 2008, someone using the pseudonym Satoshi Nakamoto published a nine-page paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System." The main problem with digital money, the author observed, was figuring out how to prevent double-spending. Digital items are easily duplicated—hence the iconic computer-age axiom that "information wants to be free." But if the recipient of a digital coin can't be sure its sender hasn't already given a copy to someone else, the coin can't be trusted.

The answer, up to that point, had been to trust a middleman instead: to channel every transaction through a financial intermediary that could check it for double-spending, mediate any disputes—and claim a cut of the action as payment. But third parties inflate transaction costs, especially for small purchases. (Think about all the mom-and-pop shops that mandate a $20 minimum for credit card swipes.) "What is needed," Nakamoto wrote, is a system "allowing any two willing parties to transact directly with each other without the need for a trusted third party."

Nakamoto proposed a solution that would obviate the need for trust entirely, by replacing it with cryptographic proof.

By using public-key cryptography, one person could securely transfer a virtual coin to another. In essence, its owner would point to the specific past transaction that had brought the coin into her possession, then digitally sign a hash of that record to transfer the coin to someone else. The digital signature is not an image of some name written in cursive, but a mathematical transformation of the message that proves it can only have come from the signer and not been altered in transit. In this way, there are no Bitcoins, only Bitcoin transactions; unlike a bank account balance, which contains the mingled sum of all your miscellaneous credits and debits, every Bitcoin transaction is a descendant of one or more specific previous ones. A recipient, call him Bob, uses software to generate a pair of cryptographically linked keys, and transforms the "public" key into a Bitcoin address to be shared with limitless senders. Alice, having already done the same, points to an address she controls, and signs it with her associated "private" key to transfer some of its contents to Bob's address.

So far, so good. But in the absence of a central authority, Nakamoto reasoned, the only way to be sure that a particular coin hadn't been spent already was to make the time-stamped record of every historical transaction available to everyone.

Broadcasting individual transactions over the internet was easy enough. The challenge was providing participants—who would be widely dispersed, uncoordinated, and collectively carrying out countless transactions simultaneously—a way to agree on a single history of the order in which transactions occurred.

Nakamoto proposed a surprisingly democratic solution: majority vote. Every proposed transaction would essentially be posted to a public bulletin board, where they could be checked against the existing historical ledger. Anybody could do the checking. In fact, an unlimited number of parties would compete as clerks, grouping what they judged to be valid transactions into blocks. When their block reached a certain size, they would broadcast it across the network—combining their batch of new transactions with a hash of the previous block, which would preserve the integrity of the chain. At that point, every other clerk could make a choice: accept the new block into the ledger, or reject it. In practice, the block would already be attached; clerks would indicate acceptance by binding their own next block to that one. If a block contained fishy transactions, they would instead latch to the preceding one, whereupon the bum block's contents would be returned to the bulletin board for further vetting.

There would be a reward for performing this work: after a block was accepted onto the chain, and several more were connected to it in turn (indicating the community's acceptance of this as the One True Ledger), it would become the source of a certain quantity of coins owned by its creator. Thus the clerks who maintained the blockchain's integrity also played a role "analogous to gold miners," introducing new coins into the monetary supply at a pre-ordained and steadily diminishing rate that, in Bitcoin's case, would culminate in 21 million coins.

As long as honest participants outnumbered dishonest ones, that should work. But what would stop a faction of malicious clerks from validating bogus, self-serving transactions? Nakamoto's answer: By making it prohibitively expensive to cheat.

If anybody was permitted to batch transactions cheaply, cheaters could spam the system with hundreds of bogus blocks, needing only one of them to squeak through in order to pull off a heist. So to qualify for acceptance, a block would require an additional piece of information: an integer that, when tacked onto the block, produced a hash beginning with a certain number of zeros.

The only feasible approach to such a puzzle would involve powering enough computers to evaluate enough guesses until a solution randomly emerged. Yet the solution would be easy to confirm. The substantial cost of generating a block (known as "proof of work") would discourage cheaters. And since each block contained the hash of the preceding one, altering a single past transaction would necessitate re-doing every subsequent block at the same time—a feat that was practically impossible.

Furthermore, even if a "greedy attacker" assembled enough computer power to overwhelm all the honest participants, using it to steal back his payments would damage his own interest. "He ought to find it more profitable to play by the rules that favour him with more new coins than everybody else combined," Nakamoto wrote, "than to undermine the system and the validity of his own wealth."

There were other wrinkles. The difficulty of the puzzle—the number of zeroes required—would be regularly and automatically adjusted such that a new block would be created roughly every 10 minutes. After the final coin is mined (sometime around 2140), clerks would be incentivized by transaction fees (which can currently be added to any transaction at the discretion of the parties involved, to incentivize miners to prioritize those transactions when assembling blocks). And the use of public-key cryptography enabled everyone to see the source and destination of every payment—but not the identity of the people controlling those coded addresses.

None of the individual elements of this scheme was new, but Nakamoto's synthesis was an elegant achievement. It enabled a currency that didn't rely on a central authority, eliminated the need for transactional middlemen, and safeguarded privacy while mastering inflation. Furthermore, its decentralized nature doubled as a discouragement to hackers; the absence of a central clearinghouse meant there would be no big "honey pot" of data for them to target, just countless isolated dribs and drabs whose contents were unlikely to justify efforts at plunder.

On January 3, 2009, Nakamoto created the inaugural Bitcoin block, which minted 50 coins. Since there were no past transactions to reference, Nakamoto used the dated text of that morning's cover headline of *The Times* of London: "Chancellor on brink of second bailout for banks."

Beyond Bitcoin

Nine and half years later, the Bitcoin blockchain has been used to exchange everything from pizza to cocaine. It has been courted by some government regulators and targeted by others. The currency has experienced dramatic rises and drops in its market value. But it has never been hacked. (Thefts have occurred, but only from third parties holding custody of Bitcoin keys.)

Considering that the price of a single Bitcoin has been as high as $19,000—giving the currency a total market value north of $300 billion—there is little doubt that many sophisticated thieves have tried to hack the chain. Their failure suggests that blockchains could be useful for securing everything from medical records, to credit histories, to digital personal identity itself—data assets that have been badly mismanaged by institutions ranging from Equifax to the federal Office of Personnel Management, and exploited by the likes of Wells Fargo and Facebook.

Then there are blockchains like Ethereum that enable "smart contracts"—lawyer-free transactions that self-execute when certain conditions are met—opening up further possibilities.

Last June, German car manufacturer Daimler AG floated part of a €100 million

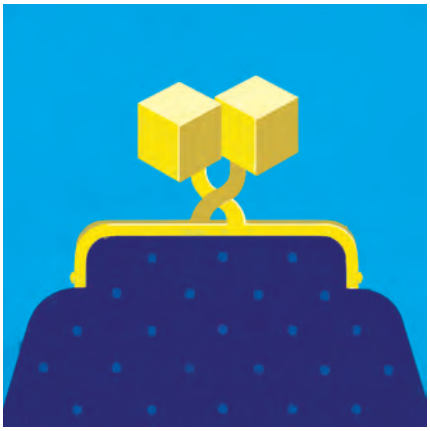
bond through a blockchain—automating everything from origination and distribution to investors to managing disbursal of interest payments. The company's head of treasury cited speed, transparency, and removing the need for a bank as benefits—and predicted that blockchains would allow for smaller and more numerous transactions in the future.

Facilitating small-value transactions is a holy grail in contemporary financial services. Asheesh Birla WG'10 is vice president of product at Ripple, a high-profile blockchain upstart. When he joined the company in 2013, he told me in January, "you could get an email in seconds, you could even beam YouTube to Mars—but if you tried to send an international payment, it was so slow and so complicated." The existing cross-border payment system was assembled in the 1960s, mainly to serve giant companies that transferred thousands or millions of dollars at a time.

"The Amazons and Ubers of the world," he said, need to pay numerous operators small sums, and they couldn't use the existing financial infrastructure without incurring prohibitive fees and cumbersome waits. The same goes for migrant workers sending money from, say, Dubai to Jordan, or the US to Honduras. Ripple has built two platforms—incorporating elements of blockchain in varying degrees (though with departures that have stoked technical arguments that lie beyond the scope of this article)—in a bid to capture that sizeable market.

Other entrepreneurs see a potential for blockchain to unleash whole new markets based on even tinier transactions. Dillon Chen's wireless-sharing idea illustrates the general concept. "We built a two-sided application," he explained in February. "One side goes on your phone or laptop, and one goes in your router: basically a gateway that accepts payments facilitated on a blockchain" via smart contracts. That would allow someone with a wireless signal to essentially sublet it, in a controlled yet frictionless way. An early iteration was

Some entrepreneurs expect blockchain to unleash whole new markets based on tiny transactions.



built to run on the Ethereum blockchain, using that currency as payment. The team experimented with creating their own token, but laid that idea aside as the initial coin offering (ICO) craze seemed to be hurtling toward an unpredictable collision with regulators (See "Bubbling Over," page 43). They also came to see their reliance on incumbent internet service providers as a terminal weakness, since Comcast or Verizon could easily quash signal-sharing by simply adjusting their terms of usage.

The project's subsequent evolution shows why some enthusiasts hope that blockchains will transform commercial activity in a deeper way. In broad strokes, Chen's team now envisions building atop what's known as a wireless mesh network—a radio-connected constellation of antennas and routers that can share a single direct connection to the internet across a geographic area. Decentralized, resilient, and unburdened by some of the infrastructure requirements of traditional ISPs, mesh networks have found use in military field operations and humanitarian disaster responses, but haven't had commercial success.

"Hardware costs for building a mesh have come down so much that someone, or a small team, can cover a particular geography," Chen says. What has been missing is a business model. A public blockchain with a native token could align the incentives: anyone wanting to use the network could buy tokens, which could be earned by anyone who wished to contribute to its expansion by adding hardware. That expansion would in turn attract further users, in a virtuous cycle whereby improvements in the network would reinforce or increase the market value of the token. No single entity would own the system, but anyone who enhanced its value could reap a reward.

That cooperative dynamic is part of what enthralls blockchain visionaries. The original internet, in their view, was a digital commons owned by no one and open to all. But its open-source protocols lacked something critical: a way to establish a stable and secure digital identity. The companies that arose to meet that need—Facebook, Google, Twitter, and the other giants of Web 2.0—have done so by creating proprietary standards: essentially, by controlling all the data that define a person's social identity. That has empowered them to build networks that derive virtually all their value from user contributions, but funnel the rewards overwhelmingly to shareholders.

Blockchains seem to offer an alternative path. They can establish digital identities secure enough to facilitate the exchange of not only information but assets. And they have an unusually broad philosophical appeal.

"For libertarians, these technologies represent economic activity outside the bounds of sovereign state control," writes Kevin Werbach, whose book *Blockchain*

and the New Architecture of Trust will be published by MIT Press in October. "For progressives, they promise to undermine entrenched private power. For others, they are simply a huge opportunity to make money or solve problems."

Danny Aranda C'08, a managing director of business development at Ripple, laid out an expansive vision during a January campus visit sponsored by the Penn Blockchain Club. "There will be a token for every single computational resource on the internet," he declared. "What that means is that for every single action that a computer, that a program, that an application needs to do, there will be a token to access that resource." As an example, he described a decentralized blockchain network called Golem. "You can plug in your computer and give your excess computing power to the network, and in return you get Golem tokens. That's the supply side. On the other side of Golem tokens are people who want computational power. Let's say I'm running some application and I want to grab some power to run some computations or algorithms. I can buy Golem tokens and now get access to that computational power distributed across that computational network. And it's all decentralized. There's no middleman taking a fee on it. There's no one abstracting or taxing value on it. It's peer to peer."

Other nascent blockchain enterprises are working on decentralized ride-sharing, online auction marketplaces, co-op services for small farmers, and music-streaming platforms enabling artists to manage their own digital copyrights, which have long been controlled by distributors. Goldman Sachs sees a multibillion-dollar market potential for blockchains to facilitate distributed electricity markets, integrating rooftop solar panels and other decentralized power generation into the grid. Others go further, forecasting the tokenization of physical assets as well: fungible goods like commodities, or fractionally owned property like apartment buildings. But even if that proves a bridge too far—Aranda professed skepticism—one can imagine blockchains being used to document the histories of physical property.

Jalak Jobanputra C'94 W'94 is the founder and managing partner of FuturePerfect Ventures, a venture capital firm that has been investing in blockchain projects since 2013. "A home's data could also be on the blockchain," she mused in a 2016 blog post: "all repairs, chain of ownership, history of electricity, etc.—providing an immutable record of ownership so that a potential buyer has all the information related to that home. The more information a seller makes available the better price she may be able to negotiate for that transaction, [creating] value for both the seller and buyer and also incentiviz[ing] owners to take better care of assets."

Given that the physical world doesn't line up neatly with the virtual one, there are likely to be limits to such schemes. But the steady incorporation of computational elements into material objects has fertilized even more imaginative ideas.

Thomas Miller G'14 spent most of the 2000s in trading and market making for foreign-exchange and derivatives. When we spoke in February, he was working for a Swiss-registered digital-asset exchange and crypto-wallet provider called Lykke (which later drew down its US operations). He believes the structure of digital-asset exchanges and custody services will play a critical role in blockchain-based commerce. To explain why, he asked me to imagine a car trip across town—as mediated by smart contracts.

Say you wanted to use an electric vehicle from a car-share service. The experience would seem simple: click *Rent* on your smartphone, listen to the door unlock, and hit the road. But behind the curtains, blockchains would be whirring: requiring one token for an hour of car time; a different one to pay some anonymous electricity supplier who charged the battery; a third to access a wireless mesh like Dillon Chen envisions; a fourth to tap into a network of geo-location beacons providing directions; a fifth to purchase mileage-based collision insurance. (And why stop there? "When the Blockchain Man gets in the car," mused essayist Taylor Pearson in an article imagining a future of self-driving cars, "he will see a sliding scale offering him the ability to set an arrival time and calculate the cost of the ride. If he wants to arrive quickly, the car will make a flurry of micropayments to other cars allowing it to pass. If he's not in a hurry, he may choose a later arrival time and lower fare, allowing other cars to fly past in return.")

Blockchain's value would be in democratizing participation in any of the underlying commercial transactions, many of which could be organized more like cooperatives than traditional companies. (Miller contends that the infrastructure for exchanging all those tokens would also need to be sufficiently decentralized. Otherwise, a single entity could—by suddenly deciding not to process trades of, say, Chen's token—strand you in traffic.)

It remains to be seen how eager people will be to turn every soccer carpool into a shifting tangle of utility-optimizing economic calculations. The impact of such systems on the digital have-nots is an open question as well. People without the means to pay for "every single computational resource" may feel that surrendering some sensitive personal data is a better deal. And do we really want blockchains enabling market forces to infiltrate even more realms of human activity than they've already conquered?

Xiao Ling was perhaps the most earnest and idealistic blockchain enthusiast I came across. We met in a crowded campus coffee shop, where he explained the cryptocurrency venture he was developing with three fellow alums and a researcher at Penn's Positive Psychology Center. Their mission was to foster meaningful offline, face-to-face interactions. When I asked him why, he looked

surprised, and simply nodded towards the next table over, where two young women ignored one another while scrolling through their Facebook feeds. Then—after surveying the room at some length—he found a pair of middle-aged men engaged in actual conversation.

"Those people know how to talk," he said, "because they're not from that generation." Ling saw his peers as having spent too much time escaping into social media to really learn how. Moreover, the painstakingly curated profiles they encountered online fostered feelings of inadequacy that further discouraged them from exposing their own unfiltered selves.

Yet Ling believed they yearned to. "People want help, but they're afraid of asking, because they don't want to appear vulnerable, or they don't know who to ask," he said. "You want to help others, but you don't want to appear presumptuous." He thought the way to decrease both points of "friction" is to introduce a third: "People like to get paid, but don't know how to ask for money, especially when it's a small amount … because it's a cultural taboo and it comes off as weird."

He envisioned a social network that would connect people seeking help—even just advice—with people offering it. A blockchain structure would help protect everyone's privacy, and offline meetings would be memorialized via nominal exchanges of a native token via smart contract—which would incentivize participation while keeping spammers at bay.

While I hated to think of a future where my warm conversation with Ling would be governed by digital supply and demand, in less lofty contexts giving people real control over their own digital information and assets could generate huge social dividends.

Blockchain Medicine

Consider the American healthcare system, where so much hope for improving outcomes and containing costs has been placed in efforts to pay for the value rather than volume of medical care.

"In the shift to value-based care, one of the biggest challenges is creating longitudinal traceability across a patient's healthcare data, and also incentives for patients to take good care of their health," said Joshua Talbot WG'18, who worked on healthcare data analytics at Deloitte. Blockchains, which create immutable data trails whose contents can be selectively shared by patients with providers, could break that logjam.

"Say you go in for a hip replacement," he said. "And over the course of 10 years, say you have some sort of a biannual checkpoint: you have someone check your vitals and verify that the hip replacement has gone well, there's been no side effects. You set up, through a smart contract, certain … milestones, and the provider is reimbursed by the payer every time you hit that milestone. So, six months in, everything is great with the patient: you get an additional payment. And all the way through 10 years down the line.

"Blockchain would enable a world where you could do that automatically, without a third party. That is hugely valuable. It enables a payer to track the progress of a patient over time, and actually reimburse the provider for value—not procedure, but value.

"And it goes both ways," Talbot added. Another smart contract could be created to release escrowed funds to a patient who fulfills certain conditions: say, attending a certain number of physical therapy sessions.

That was the thinking behind Healthcoin, which Diego Espinosa founded to incentivize diabetes prevention. "Originally the idea was to use blockchain to generate proof of prevention using actual blood lab data, and making that proof immutable on a blockchain so that it could support issuance of incentives—essentially tokens—to reward people for moving their blood labs in the right direction," he told me in February.

Yet along the way, his sights expanded—a common phenomenon in blockchain enterprises. "From the time we're born to the time we die, we generate a lot of health expression," he said, describing Healthcoin's evolution into Linnia, an outgrowth of ConsenSys, a company that develops software services atop the Ethereum blockchain. "If we could just capture this and scale it to millions of users, we could share that data with enterprises, with pharmaceutical companies, with other stakeholders, and then we'd have analyzable data that would allow us to basically have better pharmaceuticals and better prevention programs, better medical research. Accumulating that very valuable data and allowing it to flow to its best use would really benefit the system as a whole."

If that sounds like a data overlord even more powerful than Facebook, Espinosa contends that the blockchain preserves an individual's sovereignty over his or her information. A service provider, he explained, "would have some access to some types of metadata, which they could search through to say: *Hey, here's someone with these types of data, and this much of it, and it came from these great sources*." Then the provider would make its pitch: Grant us access to certain underlying data, and we'll use it to, say, broker a health-insurance policy that fits your needs better, or determine if you're eligible for a clinical trial you didn't know about. A blockchain could potentially be structured such that the company didn't

even know who it was proposing to analyze; some types of ensuing transactions could conceivably be carried out in anonymity—just as a Bitcoin user need only reveal a coded address when sending or receiving payment.

There's a host of challenges, Talbot says, to creating those sorts of metadata in a way that truly anonymizes the patient. Some years ago a Carnegie Mellon researcher found that 87 percent of Americans could be uniquely identified based only on their birth date, gender, and ZIP code. "So it will be quite an art to be able to create this second level of a blockchain in a way that gives control to the patient to push data to where it's helpful, but also allows folks like the NIH or different research organizations, or pharma companies, to essentially eliminate the CRO [contract research organization] industry entirely, which is a multibillion dollar industry that's essentially just acting as a middleman."

Data Servility and Data Sovereignty

The people I spoke with about blockchain tended to fall into one of two camps. I came to think of them as the utopians and the pragmatists. Some people swung from one camp to another, but Espinosa articulated the utopian outlook with particular passion. He concurred with Talbot's warning about the challenge of striking the right balance of privacy and transparency in blockchain applications, but framed it in even more dramatic terms.

"If you think about it," he told me, "when we lived as hunter-gatherers we kept data in a decentralized way: 150 individuals that we knew from relationships pretty much knew all about us: our location, who our social contacts were, where we were born, our health history. All this data was, in a sense, stored in a decentralized way, by that network." Over time, organizational hierarchies took over that function, and began exercising their power over our information "to get us to do certain things—some really good, some not so good." All that fundamentally changed, Espinosa declared, in 2006—with the collision of the smartphone and Web 2.0. Now "it was a few big firms that were capturing billions of data points about us, potentially over our lifetime, and using that to get us to cooperate in a way that was really nontransparent.

"Right now it may seem innocuous," he continued. "They give us these services, and we enjoy free social media, and those kinds of things. But the issue is that, increasingly, the analysis of that data is going to be used to feed artificial intelligence, and AI is going to be a much stronger influence on our lives … and it's not difficult to see how that might not head in a good direction."

As I reported this story, I started using a web browser called Brave, which allows you to see and selectively block entities that track your movement through the web. (It also gives you the option of automatically sending micropayments to websites where you spend the most time, through a smart-contract-capable blockchain that anonymizes those transactions to protect your privacy.) In one month, it intercepted more than 4,500 trackers. Whether I was visiting the *Washington Post* or *National Review*, the National Rifle Association or the nonprofit UsAgainstAlzheimer's clinical-trials page, there was Facebook, trying to log my activity—never mind that I don't have a Facebook account. Eluding Google was like trying to outrun my shadow. It was a constant stowaway on web trips to health insurers, the Susan G. Komen breast cancer page, Fox Chase Cancer Center—even when Yahoo searches led the way. ("Facebook knows a ton about your health. Now they want to make money off it," went the headline of an April *Washington Post* editorial, about a company initiative to obtain patient data from hospitals. Google, Amazon, and Apple are also charging into the "digital health" marketplace.)

Whatever ordinary people may get out this bargain, it's hard to argue with Harvard Business School professor Shoshana Zuboff's contention that we've entered the age of "surveillance capitalism."

China offers a glimpse of that future. In 2014, its government began building a system that will combine digital, biometric, commercial, and other data to assign a "social credit" score measuring the integrity of every citizen. Private companies have already implemented precursor systems that score consumers' creditworthiness on the basis of not only their bill-payment history but their educational attainment and the scores of their social-media friends. The government aims to extend that model into a "credit system that covers the whole society," enabling it to reward compliant citizens—with building permits and eased travel restrictions, say, or access to certain medical services—and punish rebellious ones.

"Those data have enormous value," Espinosa said, referring to the American context. And with blockchains, "our ability to capture that data and use it with our own agency [will] influence how we live for a long time to come."

Identity Power

Mir Haque is a utopian of another stripe. His views are shaped by his youth in Bangladesh and a restless adulthood that's taken him from driving a New York taxi, to earning a Wharton MBA, to jobs in fields as varied as cloud computing, corporate mergers and acquisitions, and immigration legal services. Like many people I spoke with, he thinks the potential for blockchains will be felt most profoundly in the developing world.

The main thing keeping his countrymen from basic financial services, he said, is a lack of economic identity. To a Western consumer seeking a car loan, or a student loan, or an apartment to rent, the biggest potential impediment is a low FICO score. But Bangladeshis face a bigger obstacle: having no FICO score (or its equivalent) at all. That's the norm throughout much of the developing world, stunting the development of entire markets.

"Eighty percent of people [in Bangladesh] have no access to bank accounts—because you don't have any identity," Haque told me. "Now, with a 10-dollar Android phone, you can leapfrog all these obstructions. You don't need a bank … you can take a selfie, and the blockchain creates a unique hash out of that image, and that hash leads to a digital identity that enables you to receive payments and remittances," and over time build a secure record you can use to obtain other financial services.

"Eventually you can do lending," he added, calling it a huge potential market that hasn't been addressed by traditional financial institutions, whose limited product offerings have carried high fees to offset the risks inherent in a low-information environment. "With a blockchain-based identity and a smart contract," he said, "peer-to-peer group lending could happen at a very low cost"—replicating a business model that companies like Lending Club have used succesfully in mature markets. "So it's lower-cost for the borrower, but the lender would get better returns than in a checking account. So there's a winner on both sides."

Ripple's Asheesh Birla also thinks the developing world has the most to gain from blockchains—and wonders if that accounts for some of the naysaying among influential figures of Western finance.

"So much of this technology is about inclusive access to the financial ecosystem." But Silicon Valley venture capitalists "have VenMo, PayPal, six credit cards—they're overbanked. They think, 'Well, I can send money instantly, what's the big issue?' But

Bubbling Over

David Crosbie knows what it feels like for a bubble to pop. Long before he became a lecturer at Penn Engineering, he was on the cusp of an IPO for a company he built during the first dot-com boom. When the tech market collapsed, his firm went "spectacularly bust." He took a philosophical view.

"I used to have a bumper sticker," he told me, "that said: PLEASE GOD, JUST ONE MORE BUBBLE."

"Why waste a good bubble?" he said. "They bring money and people and interests into a space." And as the saying goes, tomorrow's industries rise from the suds of yesterday's bubble.

Bubbles also bring headaches.

"Token sales could offer a new means of funding innovative technologies that circumvents the limitations of the traditional venture capital model," writes Wharton's Kevin Werbach. "They also offer an almost perfect way to cheat people out of their money."

A regulatory vacuum is partly to blame. So-called "initial coin offerings," or ICOs, smack of NASDAQ listings, but they have more in common with Kickstarter campaigns.

Lena Šutanovac GL'18 laments that what most of them offer shouldn't be called "coins" at all. "A coin is a currency," she told me, "whereas tokens are essentially smart contracts." Most commonly, they offer—or purport to offer, given the tidal wave of fraud out there—some sort of utility, like access to decentralized cloud-computing power. But some tokens are indeed structured more like securities, only without a watchdog like the SEC providing oversight. So, buyer beware.

The uncertainty puts blockchain developers in a bind as well.

"It's kind of the Wild West out there," said Dillon Chen W'18. "We've played it on the safe side, in terms of not doing a token offering. There needs to be oversight—there definitely needs to be a guiding hand. We need to trust someone."

Venture capitalist Jalak Jobanputra C'94 W'94 told me her firm has mostly taken equity positions in blockchain companies, but at times it has invested directly in tokens. Yet the bubble has majorly muddied the view of companies' performance and prospects.

"Token holders have gained value just from all the speculation that's happened, and the promise of what the technology may be able to do in the future," she said. "But we're still not seeing real-world implementations of utility going back out to the token holders.

"I expect a few will get there in the next year," she added.

But only if oversight agencies manage to catch up—and not overreact, Werbach contends.

"Regulation of the internet was actually an important step in its widespread adoption," he writes, noting that he was involved in that process 20 years ago. But it's tricky.

"If regulators jump in before a market is mature, they run the risk of preventing it from ever getting off the ground—and writing the rules with the old incumbent technologies too much in mind," he told me. On the other hand, if regulators wait too long, and the market grows and matures on the assumption that there are no rules, then when there need to be rules, the collateral damage can be substantial.

"Over $5 billion was raised last year in initial coin offerings," he noted. "So this is not a tiny nascent market anymore."

And it is a maddeningly uneven one. "There's a lot of crap out there," Asheesh Birla WG'10 said. "A lot of these ICOs don't have a use case. I think a lot of them are companies that raised venture equity in rounds A, B, and C, and this is a Hail Mary.

"I think the SEC will come in with strong regulation—but I don't think that's the end of it," he added. "Crypto winter may be coming for ICOs, but I do think it's going to be a fundamentally new way to raise money and digitize and tokenize assets that weren't very liquid in the past. … But the right regulatory framework needs to be applied."

Some of Werbach's prescriptions appear in a 2018 paper in *Berkeley Technology Law Journal*, "Trust, But Verify: Why the Blockchain Needs the Law," which can be found online. —*TP*

the more I travel to places like Africa, the Middle East, and other emerging markets, I realize that [these are the places] where you'll see adoption of blockchain and digital assets—because they're the ones on the fringes of the financial system."

Lena Šutanovac GL'18, a law student from Slovenia, thinks blockchains could be powerful weapons against government corruption. Blockchain-verified voting could invigorate democratic decision-making. And creating transparent blockchains for land, business, and trademark registries could eliminate bribe-heavy bureaucratic choke points that are "keeping developing democracies in a crunch and prohibiting them from developing."

And a blockchain solution to, say, consumer credit ratings may eventually prove attractive to Americans burned by the Equifax breach—just as Wells Fargo's abuse of its customers' identities sparked an appetite for alternatives. Indeed, some blockchain entrepreneurs have sloganized their mission as "unbanking the banked."

Haque, who has managed to cultivate former Mexican president Vincente Fox as an informal ally in his blockchain-related advocacy, thinks financial access could be just the beginning. Blockchains could amplify the power of education, for instance, by helping to expose fraudulent credentials and validate authentic ones. He envisions "a permanent ledger of your course completion and certification that can be authenticated from anywhere in the world"—so that a certificate in, say, PHP programming might actually carry weight with an American employer even if it was issued in French by the University of Science and Technology of Togo.

Going a step further, he imagines educational institutions administering tests and courses in the form of smart contracts on a blockchain. "You could take an exam, and get a certificate automatically assigned, time-stamped, on the smart contract," he speculated. Employers could take advantage of the same thing. "The cost of employee acquisition for a good tech developer is $25,000 to $30,000," he asserted. "That's a lot of money. One thing a company could do is give a test on a smart contract," and offer an immediate (crypto) cash reward to anyone who aced it. Even the equivalent of $100 would be "a huge incentive in a developing country. And now the employer would have a verifiable talent pool, identity authenticated—no Nigerian scam—and as a result, could contract them out for real work and reduce its costs."

Not So Fast

Even apart from the cryptocurrency bubble, there's no shortage of hype about blockchains. If some analogies point to the internet as the last comparably momentous advance, others reach all the way back to the emergence of double-entry bookkeeping in medieval Venice, which has been credited with the birth of modern commerce. Here's the problem. Blockchains, at least at present, are really, really slow. This is particularly the case with the truly open ones—like Bitcoin and Ethereum—that have generated the most excitement.

Speed, of course, is a relative concept. A blockchain that collapses the sale agreement, clearance, and settlement of

Blockchain and the Law

"In the past, people hired lawyers to review complicated contracts," opined digital-security expert Rob Graham in a 2016 consideration of blockchain's implications for legal practice. "In the future, they'll need to hire hackers."

It is a fashionable view. If distributed digital ledgers portend a "smart contract economy" in which anything from a real-estate transfer to streaming Beyoncé on your car stereo could trigger a cascade of computer codes shifting money this way and that, are traditional business lawyers going to go the way of switchboard operators?

"If all lawyers do is basically add transaction costs to processes, then it's true that they can be replaced when more efficient approaches come into being," said Kevin Werbach, an associate professor of legal studies and business ethics at Wharton. And "there are reasons why distributed ledgers would be a good platform" to automate many functions that have long been governed by paper contracts.

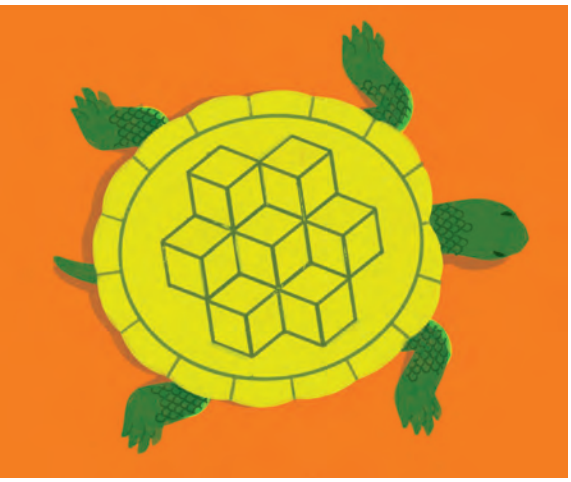
For one thing, business contracts have a lot in common with code as it is. "Most business contracts are essentially modules that lawyers string together and customize," he wrote in the *Berkeley Technology Law Journal*, "re-us[ing] standard clauses, which they adapt and negotiate for the particular transaction."

And smart contracts have already conquered some realms, like derivatives trading. Insofar as blockchains could expand the scope of such instruments, lawyers may need to master new skills.

Regulatory compliance issues won't disappear, and organizations that value a high level of legal customization will continue to pay for it. But the playing field may change, creating new niches. "We're going to see a need for a new kind of legal engineer who's able to advise companies on how to implement agreements and applications in the best possible way," Werbach said.

Lena Šutanovac GL'18 envisions a library of legal provisions formatted as code, from which such lawyers might pick and choose when structuring smart contracts. "I don't think it will ever reach the flexibility you have with paper," she told me. "But maybe we will get more legal certainty."

Yet certainty can be a two-edge sword, she pointed out. Consider a smart contract governing a multi-company supply chain involving a farm, a processing plant, a freight airline, a distribution warehouse, a short-haul truck, and a retailer. There's a lot to recommend a tool that would automate the immediate exchange of money upon each change of custody, conditional on timely receipt of goods at each phase. But



a securities trade—which currently takes about two days and multiple intermediaries—into a single instantaneous transaction represents a quantum leap in efficiency.

But other measures paint a dismal picture. The Bitcoin blockchain can currently process a maximum of 7 transactions per second. Ethereum can manage about 13. Visa's payment network, by contrast, claims the ability to handle 24,000.

Centralized databases enjoy economies of scale that decentralized ones, by dint of their massive redundancy, can never match. But the real issue lies in the time and energy required by the proof-of-work consensus algorithms that permit untrusting strangers to confidently transact with one another. As the Bitcoin network has grown, for instance, so has the difficulty of the hash puzzle at its core—which now requires so much computational juice to crack that, late last year, it was estimated that a single Bitcoin transfer consumed enough electricity to power the average American home for a week.

Some companies are experimenting with "permissioned blockchains," which, by limiting participation to parties deemed trustworthy, eliminate the need for intensive cryptographic proofs. Walmart and IBM, for instance, are piloting one to track the provenance of grocery products—which would enable the retailer, for instance, to trace and contain food contamination events far more efficiently.

Permissioned blockchains preserve the ability to create an immutable, decentralized data trail. And restricted access could make sense in many cases. Documenting the cold-storage chain of vaccines sitting in some fridge in remote Zimbabwe doesn't require universal participation. Companies will have competitive reasons to conceal many sorts of internal data on private blockchains. The law comes into play as well. "In healthcare, in finance, and potentially in shipping, where for example you're not allowed to ship to certain countries," observed David Crosbie, "you may need to have a club in order to follow regulatory practice."

"In a truly decentralized network," Werbach writes, "there is no way to impose limits on money transfers to known terrorists, transactions selling children into modern slavery, or laundering of funds known to be stolen."

Yet permissioned blockchains sacrifice the most transformative element of the technology: the ability for unknown parties to confidently transact with one another.

"One of the problems with the IBM example," Crosbie said, "is it's actually very hard to join their club. It's expensive, and you have to be vetted to get in.

---

such an instrument has, in a manner of speaking, a "mind of its own." It could be too rigid for the air freight company to pick up the phone and say, "Sorry, but a tropical storm has grounded our fleet, let's work out an alternative," or for a retailer to say, "We can't pay you because our liquidity is at a zero, can we pay you next month?"

"The contract doesn't care," Šutanovac said. "It just starts doing the steps." And as Werbach noted, there is no good way to represent terms like "reasonable" or "best efforts" in software code.

Šutanovac, a Slovenian with an undergraduate law degree from the University of Ljubljana, suggested that European businesses may be more willing than their US counterparts to embrace that level of stringency. American companies, she noted, more routinely practice "efficient breach," in which a contractual party simply stops abiding by an agreement upon determining that fulfilling it would be costlier than violating it and paying damages.

In Europe, "we have a concept called *pacta sunt servanda*, which means 'contracts are binding,'" she said. "So even if it would be efficient to breach a contact, we don't do it—because we consider the contract was an agreement, and respecting the agreement is more important than the potential outcome." Efficient breach happens occasionally in the European context, she allowed, "but it's really frowned upon, and you would go to extreme lengths" to avoid it. So abiding by smart contracts might be less of a conceptual leap.

In his law review article, Werbach explores the possible evolution of arbitration clauses to deal with disagreements arising from smart contracts. "Consider a simple smart contract in which each of the parties has a private key, and a third key is given to an expert arbitrator. The smart contract requires two of three keys in order to execute. If the parties agree the contract has been fully performed, they each provide their key and the smart contract executes. If there is a dispute, they turn to the arbitrator. She either provides her key along with that of the party seeking to enforce the contract, or refuses it and therefore prevents completion of the transaction. The system has just mimicked a legal arbitration process."

The legal system has managed to adapt to every technology from the printing press to the internet, he observed. So while blockchains may bring disruption to the legal realm, it could create as many opportunities as it destroys.

"Smart contracts are good at setting forth anticipated conditions and consequences *ex ante*, and then ensuring the consequences occur upon fulfillment of the conditions," he writes. "Legal contracts are good at cleaning up the mess when, as inevitably occurs, things do not go according to plan. There is no reason, however, that the two mechanisms cannot coexist." —*TP*

And therefore it limits the number of innovations that will happen in that space."

Jitin Jain WG'18, a co-founder of the Penn Blockchain Club, drew a broad comparison to the commercial adoption of the internet. "Big companies and organizations were quite apprehensive about putting their data in the public domain [at first], so they started moving to intranets—and *then* to the internet. It happened with cloud computing as well—incremental steps from private to public cloud computing," he said.

"I think organizations will have a tough time moving onto blockchains like Bitcoin and Ethereum, but at the same time consumers will start moving onto them for their non-critical applications," he speculated. "And by the time public blockchains have more scale and security, organizations will become more comfortable moving onto them" in search of customers. "That's the true potential."

"Scalability is a big concern," says College junior Nate Rush. "I wish everyone could just hang out until we got the perfect system, but obviously that's unreasonable. So I think there are going to be intermediate-term solutions, and then the real long-term solutions."

Rush, who projects a genuine modesty I did not necessarily expect after hearing others call him "Penn's deity of blockchain," took a leave of absence last semester to wade neck-deep in the river of coding. Over the last two years, he has made more than 1,000 contributions on GitHub, a repository of open-source code where a lot of the technical action in blockchain development takes place. He is an advocate of "proof-of-stake" consensus algorithms, an alternative to proof-of-work. Instead of solving arduous hashing puzzles, blockchain miners would instead vouch for blocks by posting cryptocurrency as collateral, which they'd forfeit if an invalid transaction was found within.

But even a good solution could prove difficult to enact. By definition, decentralized networks lack authority figures who can impose even minor changes, like when Apple automatically updates your iPhone's software. So any proposed change to a blockchain's inner workings requires either universal agreement, or a "fork" event whereby one blockchain is split in two: one of which abides by the old framework, and one of which adopts the new. That happened to Ethereum in the wake of a 2016 disagreement about the validity of a certain controversial transaction; the majority of Ethereum miners agreed to reverse it, while a minority refused, effectively becoming a spinoff chain that now goes by the name Ethereum Classic.

Jobanputra, the venture capitalist, sees other avenues for achieving scale. "Maybe because I started my venture career in tele-capital, and so have some exposure to hardware and chips, I think we're going to see lots of innovation on the hardware as well as the software and middleware," she told me. "I'm talking to entrepreneurs who are working on different ASICs [application-specific integrated circuits]. Also, if you start looking at AI and machine-learning, and adding that to some of the [new consensus proof methods emerging], you can speed up a lot of this."

Another challenge is developing tools and user interfaces that can demystify the underlying blockchains enough for ordinary people to feel comfortable using them. Bitcoin's most celebrated features—the elimination of middlemen and irreversibility of transactions—can be nerve-wracking.

For starters, humans can't memorize lengthy strings of hexadecimal code. Figuring out how to store cryptographic keys can be daunting. (That's one thing that has discouraged institutional investors from buying in, Shimon Kogan observed in his class; any single employee with access to a private key could purloin its contents and disappear, leaving his employer with no recourse to recover them.) On a deeper level, one could argue that a system requiring such extreme self-sufficiency is fundamentally anti-social. Trusting other people may be risky, but so is withholding trust. The whole reason we enter civilization is to escape the stark perils of absolute self-reliance.

"By solving this really hard, really important problem of trusting the integrity of the ledger itself, blockchain hasn't solved all the other kinds of trust problems that will come up," said Werbach. "Those who are going to use it to accomplish things need to have a more granular understanding of what their goals are, what kinds of risks they're taking on, and what kind of trust they need to engage in this kind of environment," he elaborated. "There will be, as always, segmentation in the market. Actors who are very sophisticated and able to protect themselves from risks will be able to do that. And those who are less sophisticated will have environments available to them that are more constrained, that address some of those trust concerns."

The need for trust cannot be eliminated, only displaced—and not entirely to software algorithms. "Lawyers have a role to play," said Werbach (see "Blockchain and the Law," p. 44). "Insurance entities have a role to play. Established companies that have brands and reputations that promote trust have roles to play even in a blockchain environment. Governance has a role to play. The real open question is how these different blockchain platforms and communities will develop a set of frameworks and experience to be trustworthy. And a lot of those things are about people.

"For example, the Ethereum community is very different from the Bitcoin community," he continued. "They're both using the same basic software approach, but the humans are still the things that make the difference. And I see an opportunity space for those institutions and actors who are good at promoting trust to figure out how to do that in this new environment. And that's a role for regulators too, because regulation is a way to promote trust."

The fevered activity on these and other fronts is part of what has sparked the enthusiasm of so many students, who see a rare chance to shape a virgin industry. "We're currently in the plumbing stage of blockchain," Crosbie quipped. "At the moment you can see all the guts spewed out all across the floor." Pessimists see an insoluble mess. Optimists see opportunities. Crosbie professes to be "remarkably unfussed" by the technical challenges.

"We used to have Gopher and FTP and a dozen pieces of software you put together before you could ever connect [to the internet]. And fairly quickly, what people did was hide all that. That's what Mosaic did with the Netscape browser." Sooner or later, he said, the same will happen with blockchains.

"I think blockchain will truly take root," Joshua Talbot summed up that widespread view, "when the users of a blockchain solution don't realize that blockchain is being used."

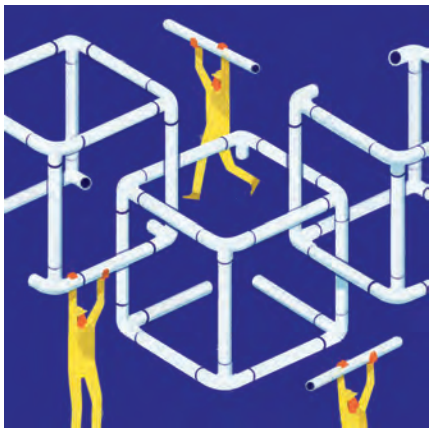
On the Varieties of Utopia

"There's blockchain as it helps business," Nate Rush mused when we spoke by Skype in February. "Then there's the other, more radical thing," he added, "and somehow that's more exciting, and also maybe more unlikely, and also really fun: … that in the long term we'll see blockchain as it replaces business."

It's a strange sort of radicalism that holds transactions to be the fundamental unit of human intercourse, and contents itself with tinkering at the intersection of supply and demand. But maybe the history of utopian schemes, spotted with failure and tombstones, argues that societies flourish most readily in the wake of more prosaic developments.

"To me," Werbach reflected, "blockchain is a foundational technical innovation that will have tremendous impacts on just about every company in the world. But that's going to unfold over a very extended period of time—and it's going to lose its purity in that process,

"There's blockchain as it helps business. Then there's the other, more radical thing: blockchain as it replaces business."



just as the internet did. Some of the wild ideas that are thrown out there are going to be interesting experiments that simply aren't going to get to scale, or are going to take much longer than people think to get to scale.

"But saying that it's just a new way to do databases is not actually derogatory," he added. "Databases are the foundation of the world economy! And if you can change the way they work in a small but real way, it has all kinds of knock-on effects."

Crosbie struck a similar tone. "You need the big vision," he said, referring to some of the wilder ideas some of his students bring him. "But I think the reality is going to be far closer to a bill of lading being put on a blockchain, and making international commerce more effective. But you shouldn't underestimate the impact on society of reducing the cost of shipping stuff around the world—given how much we ship around the world. The reality is going to be a good deal less sexy, but the impact is probably going to be greater.

"When you look at human civilization," he added, "what has generally driven growth has been the expansion of trust. Think of the Silk Road. That was largely driven by the Islamic faith, which allowed the Silk Road to operate and have trust along it." (The flow of goods and ideas along that route reached its apex under the religiously pluralistic Mongol Empire, which explicitly protected merchants and traders without regard to faith.) "Why was the British Empire successful?" he continued. "It effectively forced a system of legal structure around the world which still exists today," facilitating mercantile and intellectual exchange. Blockchains offer opportunities to expand trust even more radically.

Dillon Chen, who has traveled deep and wide in the blockchain realm since that initial prick of irritation about overpaying a local monopolist for internet access, is as good a place to end as any.

"The most impactful inventions in human history," he mused in the forum of Huntsman Hall one afternoon this winter, "have been writing, money, and then contracts and programming, if you want to lump those in. Each of those have reduced transaction costs.

"Blockchains kind of roll all that together," he continued. "And if you think of Ethereum [and its smart contracts] specifically, it kind of covers many of the use cases of a government. It's a government-in-a-box, so to speak. We pay 15 to 30 percent taxes to the government. And if we potentially can have the same level of financial stability, contract negotiation software, and money all rolled into one, with a transaction fee paid every time that adds up to, like, 1.5 percent, it's a huge step-reduction in transaction costs.

"And when costs come down by a factor of 10, a lot of interesting things happen," he said. "There's just a whole host of things that could be built that I can't even think of."