AMERICAN BANKER®
magazine
March 2014

WHY BITCOIN MATTERS FOR BANKERS

SAVVY OBSERVERS ARE LOOKING BEYOND BITCOIN AS CURRENCY AND SEEING ITS POTENTIAL AS A NEW SET OF PAYMENTS RAILS. BUT THAT'S NOT EVEN THE HALF OF IT.

BY MARC HOCHSTEIN

IT CAN BE LONELY OUT THERE FOR A BITCOIN AFICIONADO, ESPECIALLY IF YOU'RE A BANKER.

Ask Alan Lane. In October, the president and CEO of Silvergate Bank in La Jolla, Calif., was up in Sacramento for a roundtable convened by the California Bankers Association and the state's Department of Business Oversight. Reading a laundry list of about a dozen issues on the department's radar, Commissioner Jan Lynn Owen mentioned Bitcoin — the Internet currency, payment system and technology that's been grabbing headlines, igniting controversy and inspiring innovation across the globe. Lane pricked up his ears, in part because the $616 million-asset Silvergate had been in discussions about banking a Bitcoin startup.

"I raised my hand and I said, 'Is anybody else talking with any potential Bitcoin customers?' There were a lot of blank stares around the room," Lane recalls. "A lot of the bankers hadn't heard of it. … One guy, I don't remember who it was, said, 'I think they ought to outlaw it.'"

Lane's reply: "Well, if they outlaw it, I'm going to lose about $1,200 because I just bought 10 bitcoin." Later, he says, another banker friend teased him, "Uh oh, Alan, you shouldn't have said that. You just put a target on yourself with the regulators."

Lane had purchased the bitcoins with his own money, not as an investment but to experience firsthand how the system works. As Lane puts it, "How are you going to learn about this stuff if you don't step into it?"

Since that California bankers' meeting, learning about Bitcoin has seemed more and more worthwhile. At Senate hearings in November, regulators, lawmakers and law enforcement officials all acknowledged that Bitcoin has legitimate and innovative uses as a payments system. More recently, nationally known merchants like Overstock.com, Zynga and the Sacramento Kings basketball team have begun to accept Bitcoin payments. Even political candidates are taking donations through the system. Worldwide transaction volume keeps growing, as does the number of Bitcoin users.

Adam Shapiro
Promontory Financial Group

"If this becomes a valid means of exchange," Lane says, "then shame on us as bankers for not understanding it."

A true understanding of Bitcoin (uppercase "B" for the payment system and technology, lowercase for the currency) means looking beyond its potential as an alternative form of money. The network's rails one day could conceivably provide a means of exchange for a whole lot more than a stateless, digital currency — think stock certificates or property titles. For financial services, an industry predicated on trust in third parties, the long-term implications of Bitcoin's underlying decentralized technology are staggering.

MOST NEWS STORIES about Bitcoin have focused on its more tabloid-esque aspects: the currency's illicit uses in online black markets; its mysterious creator, who went by the pseudonym Satoshi Nakamoto before disappearing in 2011;

the bitcoin's wildly fluctuating exchange rate with the dollar; its adoption by celebrities like the Winklevoss twins. Online comment threads and Twitter conversations endlessly debate the red-herring question of whether bitcoins have any intrinsic value. Financial journalists view the phenomenon through a pinhole and shriek that the price is a bubble soon to burst, while the blogosphere's professional haters sneer at the libertarian leanings and somewhat fanciful predictions of Bitcoin's most passionate supporters.

Savvier observers have considered Bitcoin's merits as a global, frictionless payment system — one that offers an elegant answer to many of the questions raised last year in a paper released by the Federal Reserve, in which it called for public comments on how to modernize the country's disco-era infrastructure for moving money.

"One of the reasons we've got so many questions and why the Fed's paying attention to fixing the payment system is that there are some deficiencies in the payment system the way it stands now," says James Wester, a research analyst at IDC Financial Insights. "Bitcoin, almost by chance, it seems, has solved those problems."

For example, Bitcoin offers near-real-time settlement, something the Fed says is "desired increasingly by end users" and is "generally lacking in many legacy payment systems."

"Within 60 minutes at the longest, usually less, the money is settled, and it's settled for good," says Jeremy Allaire, the founder and CEO of Circle Internet Financial, a startup in Boston that aims to make Bitcoin easier to use for consumers and merchants. "That is radically faster than the settlement that we see in credit and debit transactions today. … From a merchant perspective it's even better because they know they got the funds. It's there."

Another item on the Fed's wish list that Bitcoin satisfies is cost reduction, particularly for cross-border transactions. Transfers from one Bitcoin address to another are free, unless the sender elects to pay an optional transaction fee, which usually amounts to pennies, for faster confirmation.

Of course, buying and selling bitcoins for fiat currency, usually through online exchanges, can carry additional costs. Even so, using Bitcoin to transmit value can end up cheaper than legacy payment methods. An analysis last year by Adam Shapiro of Promontory Financial Group found that sending $1,000 from the U.S. to Europe to make a down payment on a vacation rental would cost $15 using the Bitcoin network (including commissions paid to exchangers), compared to $50 for a cross-border credit card payment and $40 to $80 for a bank wire.

"You can't look at that and say, 'Well, that's just crazy,'" Wester says. "If it can help us address some of these issues, maybe even solve some problems, then maybe we need to stop talking about it in terms of bubbles and stuff like that."

But even this appreciation of Bitcoin is old hat. Payments aren't the half of it.

TO GET THE FULL sense of why Bitcoin matters, you have to start thinking of it not as a currency, nor as a payment system, but as a protocol — that is, a series of rules for exchange of information among computers in a network. The applications we all know and love are built on top of protocols. The World Wide Web, for example, was built atop TCP/IP, the protocol underlying the Internet.

The heart of Bitcoin is the blockchain, a decentralized, constantly updated public ledger detailing the history of all transactions on the network since its inception in 2009. The blockchain does not reside on any single server; it is maintained on thousands of computers around the world.

You've probably heard of Bitcoin "mining." The term is something of a misnomer. The job is more like that performed by county clerks, except the miners do it competitively.

Mining computers essentially race with one another to solve a complex math problem necessary to record the latest block of transactions in the blockchain. The prize for winning the race, which restarts roughly every 10 minutes, is 25 newly minted bitcoins (plus any transaction fees senders have elected to pay for faster settlement). This is why the process is called "mining," since it is how new bitcoins are added to circulation, akin to extracting gold or silver from the ground — expect instead of elbow grease, Bitcoin miners expend electricity and processing power.

There's no referee for this race. So who decides if a miner was first to cross the finish line? The other miners. They accept a new block only if all the transactions in it are valid — that is, if no one has attempted to spend bitcoins they did not have — and they communicate their acceptance by turning their attention to computing the next block. Majority consensus replaces central clearing.

By turning recordkeeping into a competition that participants anywhere can quit or rejoin at will, with a monetary incentive to take part, Nakamoto aimed to allow any two people in the world to engage in peer-to-peer transactions without relying on a trusted third party. If a miner in Oakland blows a fuse, counterparts from Iceland to Australia can pick up the slack.

"Bitcoin having no center means there's no target to attack, there's no concentration of power. Power is diffuse and distributed among the entire community,"

says Andreas M. Antonopoulos, a technologist and entrepreneur in the Bay Area who has emerged as one of Bitcoin's most fervent and articulate evangelists. "There are no levers to pull, no points to compromise. And that provides certainty for everyone."

But why should anyone trust software whose own creator is a mystery? Importantly, Bitcoin is open-source, meaning the underlying code is public information, and can be inspected by anyone.

"A geek like me can look at the source code, we don't care who wrote it," says Gavin Andresen, the chief scientist at the Bitcoin Foundation, the de facto trade association for the Bitcoin network. "Kind of like a mathematician relying on a theorem that was written by somebody they detest, you don't really care where the idea came from; you care about the idea itself."

In Bitcoin's five years of existence, "hundreds of extremely competent technical people have looked at it," Andresen says. "Both white-hat and black-hat hackers had a chance to try to break it, and nobody could."

As the lead developer for the core Bitcoin software, Andresen is probably the closest thing the community has to a figurehead. He says he and the foundation, formed in 2012, have influence, but that the governance model for Bitcoin is "very distributed, very loose," like governance of the Internet itself.

"The whole system is messy and chaotic and not top-down like a centralized system is. There's nobody who's 100% in charge," Andresen says.

And just as the decentralized setup of the Internet allowed Tim Berners-Lee to invent the Web without asking anyone's permission, the Bitcoin protocol has allowed innovative applications of the blockchain at the edges of the network.

A simple example is Proof of Existence, a notary service created by Manuel Araoz, a software developer in Argentina. The site allows anyone to embed a time-stamped cryptographic fingerprint, known as a hash, of any document into the blockchain. The user can prove later on that the document existed at a specific point in time, whether it's a will, a contract, a property deed, a patent application, a screenplay or a love letter. Storing the proof in the blockchain means there will be a permanent, ubiquitous public record of it.

To be clear: that doesn't mean exposing the document itself. Hashing is a one-way function; if all you have is the hash of a document, you can't reverse-engineer it to figure out the original data. But you can verify that a given hash belongs to a certain data set if you have both.

Even the smallest modification to the data will result in a completely different hash. Apply SHA-256, the hashing algorithm used in Bitcoin, to the word "pickle," and you get the 64 character string 6d08a4e630e4aa0d5cd873e65aea0a23df42de61073ecb49ef17158fe6a9dcea. But the plural "pickles" produces a very different string of the same length (3614e3639c0a98b1006a50ffe5744f054cf4499592fe8ef1b339601208e80066, should you be wondering).

"Having the technology provide a decentralized solution means you can trust that no matter what you're using the application for, you can trust the data anyway, because it won't be modified by any third party," says Araoz.

A more advanced idea in development is colored coins. These are bitcoins that have been digitally marked in the blockchain as carrying some secondary value. A colored coin could represent ownership of a stock, a bond, or another asset. In theory, Bitcoin could serve as the backbone for a worldwide capital market where companies could issue securities while relying less on intermediaries like clearing houses.

"You combine the decentralized nature with the open ledger and the ability for two parties who don't know each other to transact without having to have a trusted intermediary, and it really does open up the possibilities for Bitcoin being used as a way to clear certain types of asset transactions," says Barry Silbert, CEO of the New York broker-dealer SecondMarket.

Aside from dispensing with certain middlemen and bookkeepers, such a market might be more resilient. "It doesn't rely on the New York Stock Exchange, which can crash and does crash, or the Nasdaq, which can crash and does crash," says Gil Luria, an analyst at Wedbush Securities who has studied the Bitcoin ecosystem. "It relies on the distributed ledger that does not have one point of failure."

Jonathan Mohan, the founder of BitcoinNYC, a Bitcoin community networking group in New York, likens colored coins to a stamped envelope — the bitcoin is the stamp that enables the contents of the package to travel through the postal system. Looking at the recent price of bitcoins, you might think $800 is pretty steep for a postage stamp. But bitcoins are divisible to the eighth decimal point. So an issuer could conceivably acquire a thousandth of a bitcoin for 80 cents, tag it as a stock or bond, and then subdivide it into smaller bits for distribution to investors.

Even more imaginative potential uses of the blockchain involve the interrelated concepts of smart property, smart contracts and programmable money.

In the basic Bitcoin transaction, if Bob wants to send Alice a bitcoin he needs two pieces of information: his private key, and an address generated from her public key. Anyone can send money to a Bitcoin address, but only a signature generated by the private key can release money from it.

But what if the private key were a car key? A car owner or a

rental company or a lender could configure a vehicle to turn on only if it receives a message signed by a private key that owns a colored coin.

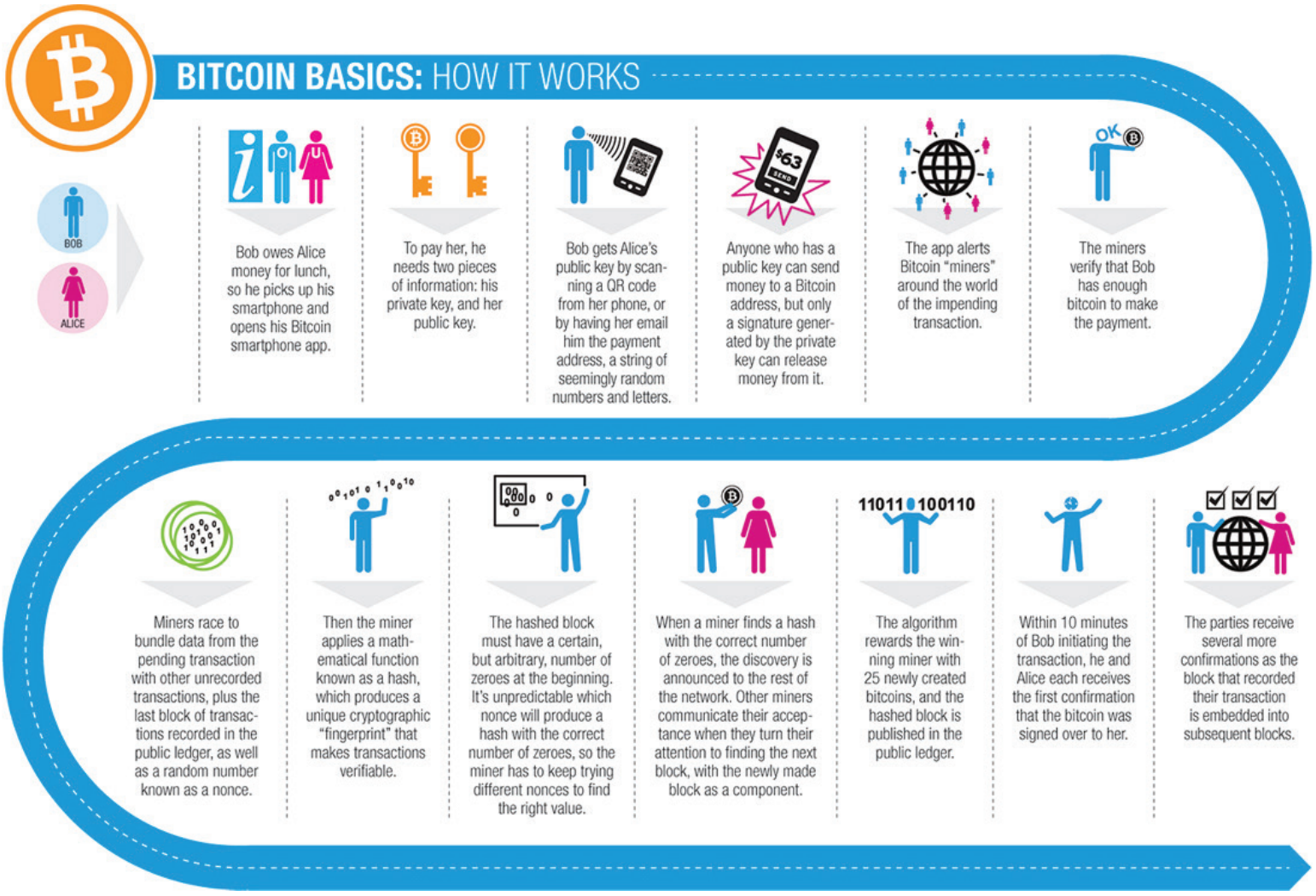
"Were I to borrow money in order to buy a Tesla," says Luria, "as long as I make my payments, that would be reflected by my bank to the blockchain and I would be able to continue to operate my vehicle. But were I to stop making payments on my car, instead of lawyers and debt collectors and repo men getting involved — if the blockchain was not to receive a message from the bank that I'd made my payment that month — they could disable the Tesla and quite directly prevent me from operating it."

And since everything would be recorded in the blockchain, both parties could see exactly what happened, and neither side could deceive the other. No more "check's in the mail" excuses from borrowers; no more predatory acts by creditors, like failing to post a consumer's payments in a timely manner.

And the borrower needn't sacrifice privacy. Since Bitcoin addresses are pseudonymous alphanumeric strings, outsiders looking at the blockchain wouldn't necessarily know who the parties are. All that would be visible is how many bitcoins have moved from A to B and when.

Antonopoulos envisions Bitcoin eventually enabling a new field of "computational law," in which contracts — which could include loans, asset sales or service agreements — are written as largely self-executing computer programs, and much of the counterparty risk of business simply disappears. That, Antonopoulos says, would leave lawyers "much more focused on capturing and expressing the desires of the parties [in writing the scripts] rather than settling the disputes or arbitrating the disputes on the back end."

THAT'S A LONG WAY off, of course. As Lane witnessed



at the California banker meeting, most U.S. banks are still wary of participating in the Bitcoin economy even in the most mundane way: opening deposit accounts for virtual currency exchangers.

"Every Bitcoin business has had at least one bank account shut down on them," Tony Gallippi, CEO of the Atlanta payment processor BitPay, said at a conference last summer.

For many bankers, guidance released last year by the Treasury Department's Financial Crimes Enforcement Network, which subjected virtual currency firms to the same know-your-customer requirements as traditional money services businesses, hasn't sufficed to remove the scarlet "A" (for anonymity) from these startups.

"The challenge here with a lot of the reluctance of financial institutions to provide banking services for Bitcoin companies, it's because they need guidance from the regulators, too," says Bruce Wallace, the chief operations officer at SVB Financial Group, parent of Silicon Valley Bank in Santa Clara, Calif.

As you might expect from its name and location, this $22 billion-asset bank is more favorably disposed than most to working with innovative companies and has a handful of virtual currency clients. But it's not taking on any more.

"We're challenged a little bit right now," Wallace says. "We need to spend more time on trying to help regulators, trying to figure out the right guidelines here with companies as opposed to spending more time figuring out how to bank more companies."

One issue that federal regulators need to clear up, he says, is how far a bank is expected to go in monitoring its customers' customers after they convert their dollars to virtual currency or vice versa.

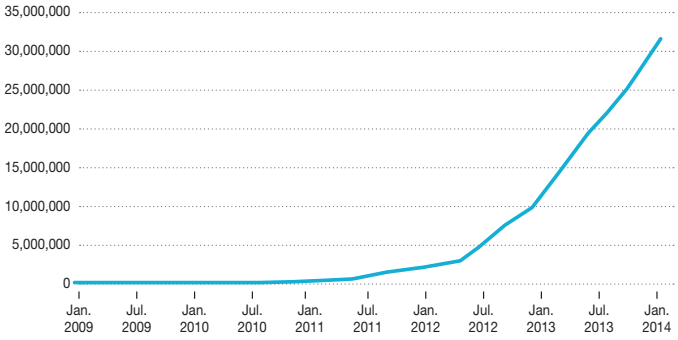
"Today, if a consumer went into a bank, and they withdraw $5,000 in cash, the bank is absolutely required to know that they took $5,000 in cash. But then, what they subsequently do with that, it would be impossible for the bank to know," Wallace says.

Bitcoin, which has characteristics of both cash and electronic funds transfers, does not cleanly fit into either category.

"When you can't see who they're exchanging the bitcoin with, when all you can see is it's just a wallet address," Wallace says, "it's difficult for a financial institution to say, 'Yes, we can confidently report that we saw that transaction happen and we saw that the other side of the transaction was with a legitimate third party that we know the identity of, and we know the reason that they did that transaction.'"

With the blockchain offering a trail of crumbs, it's ambiguous as to whether banks need to follow it or treat a bitcoin purchase like an ATM withdrawal. (Wallace says he doesn't have a preference which side the regulators come down on, as long as they provide clarity.)

TOTAL NUMBER OF BITCOIN TRANSACTIONS



Source: blockchain.info

But further regulation, warranted or not, presents a risk to Bitcoin achieving its full potential.

"No one government can shut Bitcoin down. No one regulator can shut Bitcoin down," says Luria at Wedbush. "But what governments and regulators can do is impede the progress and the innovation, especially in their country."

Price volatility is another impediment to Bitcoin's adoption as a payment system. Processors like BitPay and Coinbase have made this issue manageable for merchants by immediately converting bitcoin payments to dollars for them, for a fee that still beats the credit card companies. But not knowing how much a currency will be worth from one day to the next could hinder adoption by consumers outside a core group of speculators, curiosity seekers and die-hard Bitcoiners.

"Volatility is definitely an issue and definitely a problem," says Andresen at the Bitcoin Foundation. "For it to really be a viable payment system, you do want it to be much more stable than it's been."

Is stability attainable for a currency that, unlike most others, is not supported by any government with the power to tax its citizens (or "backed by men with guns," in economist Paul Krugman's memorable phrasing)? Allaire at Circle Financial says the price could stabilize if institutional investors start to get involved. Silbert's firm, SecondMarket, launched the Bitcoin Investment Trust last year for accredited investors; the Winklevoss brothers, famous for their wrangling with Mark Zuckerberg over the genesis of Facebook, are still awaiting SEC approval for their proposed bitcoin exchange-traded fund.

As a payment system, Bitcoin offers an attractive safety feature in that it is a "push" system, requiring an active step by the accountholder each time a payment is triggered. Contrast this to "pull" payments, where the consumer gives

a credit card or bank account number to a merchant or recurring biller, trusting that this third party will safeguard the information. Security breaches like the one Target suffered during the holiday shopping season highlight the advantages of a push-only system.

But there are other potential weaknesses in the Bitcoin network. Probably the biggest long-term risk to the system is the possibility of a "51% attack," in which one entity takes over the majority of mining power and wreaks havoc, perhaps by double-spending coins or preventing other users' transactions from being processed.

Mining already has strayed from Nakamoto's vision of "one CPU, one vote." As the business grew more competitive, miners formed pools, manufacturers introduced powerful chips, known as ASICs, designed specifically for mining bitcoins, and the math problems became more difficult. The last year saw a couple of close calls in which a mining pool came close to controlling 51% of the processing power on the network. Realizing that the value of bitcoins depends on Bitcoin being controlled by no one, the pool wisely cut back each time.

"There's so much vested interest by all the participants for Bitcoin to be successful that even when we approach these types of levels, the system wants to self-correct so as not to cast the whole network in doubt," Luria says. "Absolutely this could be a point of vulnerability, but at least for now the stakeholders are trying to manage that risk and steer clear of it."

Andresen predicts that eventually mining chips will become cheap and plentiful, after manufacturers engineer them down to the tiniest, most energy-efficient size possible. "These chips will become ubiquitous. You might buy a box of Cracker Jacks and get a Bitcoin mining ASIC unit," he says. "Just doing that will make mining much less centralized and much more … 'one mining chip, one vote.'"

EVEN IF BITCOIN GETS taken over by a malicious actor, or is crippled by governments or by a price collapse, the idea is here to stay.

There already has been a proliferation of other blockchain-based cryptocurrencies. As of mid-January, the website Cryptsy listed 117 "alt-coins." Many of them appear to be pump-and-dump schemes, or spoofs like Dogecoin (named after an Internet meme featuring a Shiba Inu dog) and Coinye West (self-explanatory for anyone even vaguely familiar with either rap music or Kim Kardashian's latest romance). But some crytopcurrencies, like Ethereum, which boasts a more sophisticated underlying programming language than Bitcoin, are apparently serious endeavors being designed specifically for advanced, smart-money applications.

Antonopoulos compares the invention of the blockchain to nuclear fission. "There's the discovery of fission, then there's building an actual nuclear reactor and then there's the electricity that comes out of it. And everybody's focusing on the price of the electricity that's coming out of it, and they're missing the point that fission in itself changes physics, changes energy, changes everything, really. Maybe you can ban electricity, maybe you can regulate reactors. But you certainly can't make people forget that fission exists. And you can't make that discovery disappear."

As for Silvergate's CEO, Lane, he isn't banking any Bitcoin startups yet but he says he's been talking with Coinsetter, a virtual currency exchange with a compliance program he finds impressively rigorous. "If we can figure out a way to do it and we can get our regulators comfortable with it, we'd be all for it," he says.

Lane doesn't expect too many of his peers in banking to become as quick a study on Bitcoin. Even he finds it tough to carve out time to explore it and has yet to do much with the bitcoins he bought. "There are a lot of things that a bank CEO has to worry about," Lane says. "I don't begrudge anybody if they say, 'Hey, if that really takes off, I'll learn about it but I can't chase every fly-by-night idea.'"

Still, "of all the things you might get interested in in a given day," Bitcoin, he says, "touches all the things I'm interested in, in terms of finance, technology, payments, and I said, 'I should learn more about that.' The more I learned, the more I said, 'Gosh, this is pretty cool.'" ▪

Marc Hochstein is American Banker's executive editor and oversees BankThink, a blog about ideas in financial services.