

Coinbase founders **Fred Ehrsam**, left, and **Brian Armstrong** in their San Francisco headquarters



REINVENTING MONEY

BITCOIN

FOR THE

REST OF

US

HOW THE FOUNDERS OF COINBASE  
ARE DEMYSTIFYING, UNCOMPLICATING  
AND OTHERWISE MAINSTREAMING  
THEIR FAVORITE CRYPTOCURRENCY

BY ANTHONY EFFINGER

PHOTOGRAPHS BY DAN MONICK

JPMorgan Chase & Co. show how the old forms of payment and transfer are ripe for replacement, bitcoin believers say.

Coinbase is a bitcoin blue chip. Armstrong and Ehrsam have scored money and support from Y Combinator, the hyperselective startup booster in Silicon Valley. New York-based Union Square Ventures led a \$5 million investment in May 2013, and Marc Andreessen's Menlo Park, California-based venture capital firm, Andreessen Horowitz LLC, anchored a \$25 million B round in December.

Andreessen may be more stoked about bitcoin than anyone else in techdom. He says it fills a void in the Internet that has existed since he and his friend Eric Bina invented the first widely used Web browser in the 1990s: a protocol for payments. He always imagined that someone would figure out how to send money as easily as data. (Bloomberg LP, the parent of Bloomberg News and *Bloomberg Markets*, is an investor in Andreessen Horowitz.)

the largest bitcoin exchange in the world, collapsed, and suddenly 850,000 bitcoins, worth \$500 million at the time, were just ... gone. (Two hundred thousand of the missing bitcoins later turned up.) Before and since, there have been numerous bitcoin heists, blamed on hackers, and more than a few bitcoin losses—people literally lose their bitcoins by misplacing the code that proves ownership. If you do that, there's no reset, no more than if you drop a \$100 bill through a sewer grate.

"Right now, it's just about making people feel safe and secure," Ehrsam says in an interview at Coinbase's headquarters. Coinbase looks like a startup, with rows of industrial-sized Apple computers on Ikea tables, except that it's on the 26th floor of a building in San Francisco's financial

## COINBASE LOOKS LIKE A STARTUP, EXCEPT THAT IT'S ON THE 26TH FLOOR OF A BUILDING IN SAN FRANCISCO'S FINANCIAL DISTRICT, NESTLED AMONG THE VERY BANKS BITCOIN LOVERS LOVE TO HATE.

district, nestled among the very banks bitcoin lovers love to hate.

Bitcoin is worth a makeover, Armstrong and Ehrsam say, because the currency solves so many problems that come with putting old technology, in particular credit cards, on the Internet. When consumers use bitcoins, merchants pay fees that are a fraction of what credit card companies get. Users can shop online without giving their names, never mind credit card information—which, yes, explains Silk Road but also allows noncriminals to claw back some privacy. As for security, the bitcoin system has thwarted every attack thus far. Recent hacks of Target Corp. and

Like many West Coast entrepreneurs, Armstrong and Ehrsam relish cutting out financial middlemen and have a special scorn for credit card companies. In Armstrong's view, they entice customers with airline miles, then fleece merchants with fees. "This is the way they're innovating, playing these games," he says.

Such fees add up to a big opportunity for bitcoin. Credit card and debit fees in the U.S. totaled \$72 billion in 2013, says Gil Luria, an analyst at Wedbush Securities Inc. in Los Angeles. Much of that could vanish if bitcoin catches on, he says.

Bitcoin arrived in the world on Halloween 2008 in the form of a nine-page

# B

## RIAN ARMSTRONG

and Fred Ehrsam certainly look like the kind of guys who could help bitcoin recover from its wild years.

They are tall and textbook fit, and as poised as Swiss bankers—Vulcan Swiss bankers. Armstrong, 31 and a former software engineer at Airbnb Inc., shaves his head. Ehrsam, 26 and a former foreign-exchange trader at Goldman Sachs Group Inc., keeps his hair short and very much in place. When they discuss bitcoin, they rarely smile. Do not try to make them laugh.

Their seriousness is understandable. Armstrong and Ehrsam are the founders of a startup called Coinbase Inc., whose mission is to convince everyone that bitcoin isn't an Internet scam or a libertarian plot against the government or a digital version of goldbuggery, as various skeptics have it. Rather, it's the best thing to happen to money since the Lydians started minting coins sometime in the seventh century B.C.

Coinbase isn't a bank—technically, it's a brokerage—but in important respects it behaves like one. Customers open accounts, through which they buy bitcoins for dollars. Coinbase holds the bitcoins. Customers spend them using a computer or a smartphone application. Coinbase makes money by charging a 1 percent fee for exchanging dollars and bitcoins. All other transactions are free.

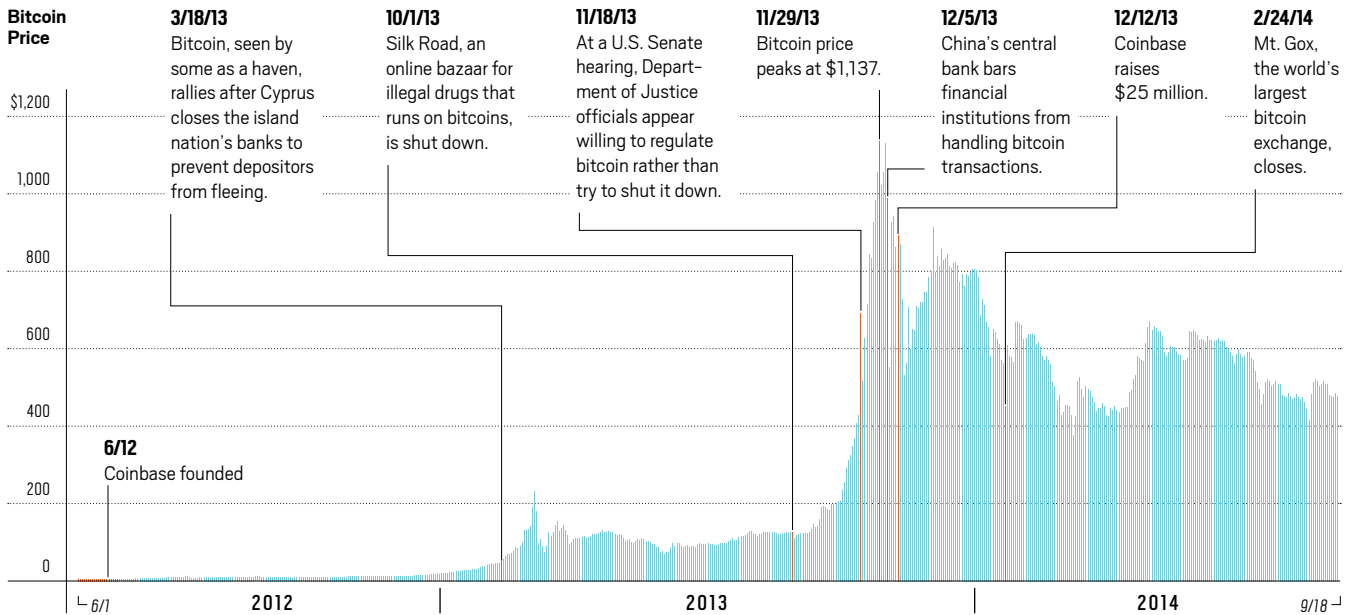
Coinbase's aim is to take a curio currency that exists only as bits on the Internet and turn it into a coin of the realm—every realm, because part of the appeal of bitcoin is that it can cross borders as easily as e-mail.

It's a big job. Reputation is everything when it comes to currency, and bitcoin's has taken some hits.

In 2013, the FBI busted Silk Road, an online drug market that ran on bitcoins. In February 2014, Tokyo-based Mt. Gox, once

# HOLD ON TIGHT

BITCOIN'S EXTRAORDINARY VOLATILITY CAN ONLY SOMETIMES, AND ONLY SORT OF, BE EXPLAINED BY EVENTS.



white paper called “Bitcoin: A Peer-to-Peer Electronic Cash System,” authored by Satoshi Nakamoto, a person or group of people who remains anonymous. Nakamoto unleashed the bitcoin software, all of it public, in January 2009. The system allowed for the creation of 21 million bitcoins, total, with the last ones to be released in 2140.

Bitcoin lets commerce happen without an overarching authority, be it a bank that clears transactions or even a central bank that controls the money supply. It works because each bitcoin is really just a slot in a huge, peer-to-peer online ledger—millions of slots, really, because each bitcoin, worth \$417 as of Sept. 18, is infinitely divisible. The smallest unit so far, eight places beyond the decimal point, is called a Satoshi. It was worth about 0.0004 cent as of Sept. 18.

Electronic currencies had been proposed before, but no one could figure out the double-spending problem: You can't spend the dollar in your friend's pocket, but you could spend the same electronic

dollar twice if you gave it to two people at the same time.

Nakamoto found a solution. No bitcoin transaction is legitimate unless it comports with all of the preceding transactions for each bitcoin involved. Every transaction for every bitcoin is available to every computer that joins the peer-to-peer network that runs the bitcoin system. Buy a watch on Overstock.com, one of the biggest retailers to take bitcoins, and the system goes to work, checking the common ledger for past transactions that prove you have the money. The purchase isn't done until all the computers on the network agree.

Why does anyone devote any time to checking transactions? Because programmers earn new bitcoins for the work—if their computers also find, by trial and error, the solution to a complex equation that the bitcoin system automatically makes harder as more computing power goes to work on it. This hurdle is designed to prevent a rogue programmer from hijacking the system. Taken together, the

checking and solving is called mining bitcoins. In the beginning, people were able to mine bitcoins on desktop computers. Now, it takes huge rigs built on special chips and running in places, such as Iceland, where the electricity needed to power the machines is cheap.

That magical ledger is called the *blockchain*, and there is no word more exciting to Silicon Valley venture capitalists these days. Andreessen and others say the blockchain could be used to keep track of not just money but anything that needs third-party verification, such as real estate contracts or stock trades. It might even track voting and guarantee one ballot per person. On a website called Proofofexistence.com, it's possible to turn a document like a lease, or even a novel, into a hash—a code generated by an algorithm—and load it into the bitcoin blockchain, proving that it existed at a certain time.

Alec Ross, until last year the senior adviser for innovation at the U.S. State Department and now a consultant, says he loves blockchain technology, but he isn't

**Adam Draper** wants to fund 100 bitcoin-related companies at his accelerator, Boost VC.



convinced about bitcoin. One basic problem: “The unit is ridiculous,” he says. At \$417 per bitcoin, it’s too big. Just because it’s divisible into tiny pieces doesn’t mean people will be comfortable with tiny pieces. “It’s an important innovation in computer science,” Ross says. “I just don’t think it’s necessarily going to supplant the euro.”

Armstrong was an early adopter of bitcoin technology. After growing up in San Jose, California, he graduated from Rice University with bachelor’s degrees in economics and computer science and a master’s in computer science, all in 2005. He worked in information technology for Deloitte & Touche LLP and then returned full time to a company he had founded in college, called UniversityTutor.com. He joined Airbnb, the online lodging company, in 2011, and set to work building the company’s anti-fraud system.

While there, he saw how hard it was for

Airbnb to handle payments from around the world. Then he discovered the Nakamoto white paper and was dazzled. Here was a currency that could fly across borders via an e-mail. Proficient in a babel of computer languages, he built a digital wallet to hold bitcoins on Android phones. Already, the idea was to make bitcoin accessible, to mainstream it.

He thought there was a company in this. He applied to Y Combinator. The founders of Airbnb and Reddit Inc. went through Y Combinator, as did Justin Kan, founder of the gaming platform Twitch Interactive

Inc., which Amazon.com Inc. bought in August for \$970 million.

Armstrong won a spot in the 12-week Y Combinator session that began in April 2012. Fred Wilson from Union Square Ventures was there doing office hours and met Armstrong. Until then, Wilson says, all the bitcoin guys seemed like ideologues: conspiracy theorists keen to escape what they see as the tyranny of institutions such as the U.S. Federal Reserve. “He didn’t have a hard-core libertarian bent,” Wilson says. “He was focused on solving pragmatic problems with bitcoin.”

**THE FIRST BIG CHALLENGE TO ADDRESS WAS HOW TO BUY BITCOINS EASILY. IT WAS HARD TO TURN DOLLARS, OR ANY OTHER CURRENCY, INTO BITCOINS.**

Armstrong finished Y Combinator that June, formally launched Coinbase and went looking for money. He called on Adam Draper, son of venture capitalist Tim Draper. Adam was in the midst of starting Boost VC, a Y Combinator-like accelerator in San Mateo, California. He wanted to invest across categories but

also to develop a specialty. “We looked at drones,” he says. “They’re cool, but there are two use cases: One is taco delivery, and the other is national security.”

Draper had heard about bitcoin. Its promise became apparent, he says, after he met Armstrong at Red Rock Coffee in Mountain View, California, a hangout for

caffeine-seeking coders. They talked amid the clicking of keyboards. After hearing Armstrong out, Draper invested his own money in Coinbase and six months later decided to have Boost focus on embryonic bitcoin companies. He wants to fund 100 of them.

The first big challenge Armstrong addressed was how to buy bitcoins easily.



# SEEING IS BELIEVING

**DOLLARS, EUROS AND POUNDS ARE** easy to visualize: They’re physical objects. Being digital, bitcoins aren’t tangible—which has become a boon for George Frey. “I’ve sort of cornered the market on bitcoin photos,” says the Provo, Utah-based photographer.

Indeed, dozens of media outlets, including Bloomberg News, have published Frey’s pictures. The image used here—dated April 26, 2013—happens to rank as the most popular bitcoin photograph on Gettyimages.com. But if a bitcoin isn’t a physical object, what exactly are we looking at in Frey’s photographs?

They’re called Casascius bitcoins, and they were minted, in a variety of metals, by software engineer Mike Caldwell at his home in Sandy, Utah. An early bitcoin adopter, Caldwell wanted

to help popularize the cryptocurrency—but he, too, grappled with its intangibility. “No one is going to get this if I can’t show them something,” Caldwell remembers thinking. So in September 2011, he began making physical coins as vessels. Inside of each, he embedded a piece of paper that contained a bitcoin private key, which he protected with a tamper-resistant hologram sticker. As for the word *casascius*, it was half acronym (derived from the phrase “call a spade a spade”), half Latin-sounding suffix (“cius”).

As of Nov. 27, 2013, however, Caldwell no longer includes digital bitcoins in his physical bitcoins. A letter from the U.S. Treasury Department’s Financial Crimes Enforcement Network, or FinCEN, stopped him in his tracks: FinCEN considered his activity

to be money transmitting and informed him that he lacked the necessary license. Since then, Caldwell has sold only aluminum promo coins via his website, Casascius.com. A bag of 500 costs 0.39 bitcoin—about \$163 as of Sept. 18. All told, Caldwell minted about 60,000 Casascius bitcoins. Bitcoin enthusiasts consider them collectibles—especially the earliest ones, which have fetched as much as \$2,500 each on EBay because of a typo in the hologram.

Not that much of this matters to Frey, whose photos continue to be downloaded via Getty. Frey says he’s made more than \$10,000 off the images, which he shot at Caldwell’s home. Unlike Caldwell, he accepts only U.S. currency for his work.

**JOEL WEBER**

Back then, buyers and sellers gathered in parks or bars to trade cash for bits. Others wired money to brokers, often abroad, and hoped. It was hard to turn dollars, or any other currency, into bitcoins.

Armstrong solved that by gaining access to the Automated Clearing House, or ACH, the electronic rails on which certain financial transactions run in the U.S. Employers use ACH to deposit checks in employee accounts, for example. To get on, a company needs a bank to sponsor it. Bitcoin companies struggle, Armstrong says, because banks worry that with bitcoin, you can't know your customer and prevent money laundering, two things regulators require.

Armstrong scored a banking relationship with Silicon Valley Bank in October 2012. A month later, customers could

## EHRSAM CAME ACROSS ARMSTRONG'S WORK. HE STARTED BUYING AND SELLING BITCOINS, SOMETIMES ON HIS PHONE FROM THE BATHROOM AT GOLDMAN SACHS.

transfer money from a U.S. bank account to Coinbase and buy bitcoins. No muss, no fuss. Circle Internet Financial Ltd., a Boston-based bitcoin brokerage, also offers ACH transfers.

In New York, Ehrsam had fallen under Nakamoto's spell. It happened when a friend from Duke University, where Ehrsam had studied computer science, pulled up the white paper. Ehrsam read that and

then everything else he could discover about bitcoin. "You could find nobody in person who could explain how bitcoin worked," he says. He came across Armstrong's work on the Internet. They corresponded, and Ehrsam started buying and selling bitcoins, sometimes on his phone from the bathroom at Goldman Sachs. "We traded it for fun and some profit," he says.

Ehrsam flew to San Francisco and met

# HEDGING BITCOINS

**CHRISTIAN MARTIN AND LEONARD NUARA** go to a lot of bitcoin conferences, and, at 49 and 55, respectively, they invariably feel old. "Everyone else is 25 and good-looking," Nuara says.

The graybeards are trying to help bitcoin grow up. Their company, TeraExchange LLC, runs the first regulated trading platform where people can shed some of the risk of owning bitcoins.

And there's a lot of risk to owning bitcoins. Imagine your business accepts it, and on Friday, Feb. 21, you made a big sale. You didn't sell your bitcoins for dollars that same day. On Monday, you found the value of your bitcoins had plunged 20 percent during the weekend.

That's why Martin and Nuara are bringing an old-fashioned idea to the hip new currency: hedging. They worked for seven months to develop a U.S. dollar-bitcoin swap contract and

register it with the U.S. Commodity Futures Trading Commission.

Now, a merchant looking to lock in today's bitcoin price can use Tera's system to find a buyer willing to pay that price in 30 days or 60. So far, the buyers—usually bitcoin-focused hedge funds or other speculators—are willing to go out about four months. Beyond that, the currency is too volatile. In the first eight months of 2014, it ranged from \$376.90 to \$914.51. "I don't expect anyone to be making markets in bitcoin out two years anytime soon," Martin says.

Martin and Nuara are old school. Martin spent 20 years at Merrill Lynch & Co. and its parent, Bank of America Corp. Nuara, a lawyer, worked at Greenberg Traurig LLP.

Some of the young guns are hot to hedge, too. Early this year, Matt Slater, 23, co-founded a company called Hedgy Inc. with former Apple Inc. engineers

Juan Pineda and Tim Olson, and designer Warren Paul Anderson. Hedgy is building a system to hedge bitcoins via the blockchain, bitcoin's beating heart and what even skeptics call its greatest strength.

The blockchain is an online ledger that tracks all bitcoin transactions. It can also be used to prove the existence of contracts at certain times and terms. Bitcoin sales arranged by Hedgy and set for a future date will be encoded in the blockchain. Both sides of a trade will put 20 percent of the value of the contract in escrow—again in the blockchain.

As the bitcoin price moves in either direction, the blockchain will make a payment from escrow to the other party automatically. No party will be able to remove that collateral.

TeraExchange's platform is up and running. Hedgy is looking for venture capital. Old and new solutions to the same problem: how to take some of the risk out of owning a strange new asset with plenty of promise.

**ANTHONY EFFINGER**

Armstrong at The Creamery, a coffee shop popular with techies because it's near the Caltrain station, where people arrive from Silicon Valley for meetings in the city. Both were a little guarded, Ehram recalls. "I could tell that the mental horsepower was there," Armstrong says. "We decided to work on something for a week."

They hit it off, and Ehram joined Coinbase in November 2012, taking the title of co-founder. Back then, some 15,000 people had wallets on Coinbase, and they bought and sold about \$1 million in bitcoins a month, Armstrong says. He and Ehram ran the thing by themselves out of a two-bedroom apartment in San Francisco. At the time, one bitcoin sold for about \$13. People still used a whole one to buy a pizza, if they could find a shop that accepted it.

The price of a bitcoin rose for most of 2013, peaking at \$1,137 on Nov. 29. By year's end, Coinbase had more than 600,000 users, and it got a further \$25 million from venture capitalists, with Andreessen Horowitz putting in the biggest chunk.

The success of bitcoin, and Coinbase, will depend in part on whether big merchants start accepting it. Armstrong

and Ehram are pitching them. So far, they've convinced computer maker Dell Inc., travel company Expedia Inc. and software maker Intuit Inc. to take bitcoins and to open merchant accounts on Coinbase.

The system will have to prove secure, too, for the general public to get on board. Bitcoin "manages to function in a very adversarial environment," says Paul Kocher,

## BITCOIN SEEMS AS FUTURISTIC AS A LIGHT SABER UNTIL IT COMES TO KEEPING HOLD OF THE PRIVATE KEY. THEN IT SEEMS AS ANCIENT AND CLUNKY AS GOLD.

president and chief scientist at Cryptography Research, a part of semiconductor designer Rambus Inc. By that, he means that everyone wants to attack it, because it's money.

Bitcoin uses something called public-key cryptography, which requires two keys, each a string of numbers and letters. One is public and identifies the sender or recipient in a bitcoin transaction. The other key is private and is used to verify, or sign, the transaction. Unlike a Facebook password, the private key can't be retrieved with an e-mail if it's lost. Once it's gone, it's gone.

Bitcoin seems as futuristic as a light saber until it comes to keeping hold of the private key. Then it seems as ancient and clunky as gold. Fearing hackers, many people print out their private keys, delete them from their computers and put them in safes. Many a bitcoin has been lost to hard drives crashing, according to the U.S. Consumer Financial Protection Bureau.

"For the average consumer, bitcoin is a risky proposition," says Mercedes Tunstall, a partner at law firm Ballard Spahr LLP in Washington and an expert on data security. Hackers can get private keys off a person's computer, she says, because people don't protect them properly. "If you and I are walking down the street with cash in our pockets, we know how to keep

it out of view," she says. "With bitcoin, there is no way for the average consumer to protect themselves."

Coinbase addresses that by keeping everything in house. Coinbase users never even see their private keys. They just have accounts with passwords, and those passwords are backed up with ever-changing codes sent to their phones. Coinbase, in turn, puts many of the bitcoins it holds in

what the company refers to as *cold storage*. It splits individual private keys, writes them onto USB drives and prints them on paper, and puts everything in vaults and safety deposit boxes at various locations. No one person can retrieve the codes. "We don't want someone to come in here, kidnap Fred and me and get a quorum of these keys," Armstrong says.

Many bitcoin lovers, Ehram and Armstrong included, make endless comparisons between e-mail and bitcoin. One sends data, the other money. People freaked out about the security of e-mail in the beginning, and today they send all manner of private information electronically because it's proved easy to use and secure, provided basic security protocols are observed.

Armstrong and Ehram say the same thing will happen with bitcoin. The chance for merchants to avoid credit card fees of 2 percent to 3 percent and the ability to send money for free, anywhere, will attract more and more users, and more and more merchants, they say. What seems strange and scary now will become familiar, and bitcoin will go from curio to currency. That's the bet Armstrong and Ehram are making, with deadly seriousness.

**Anthony Effinger** is a senior writer at *Bloomberg Markets* in Portland. [aeffinger@bloomberg.net](mailto:aeffinger@bloomberg.net)

### BLOOMBERG TIPS

#### Tracking Bitcoin

You can use the Virtual Currency Monitor (VCCY) function to track bitcoin prices. Type **VCCY <Go>** on the Bloomberg Professional service to display prices from Coinbase as well as from bitcoin exchanges Bitstamp Ltd. and Kraken. Click on Coinbase to display an intraday chart of prices from the exchange. For Bloomberg Intelligence research pieces relating to bitcoin, type **BI CARD <Go>** for the Credit & Debit dashboard. Click on Themes on the left side of the screen under Analysis and then on the piece entitled "Bitcoin: Disruptive Technology or Novelty?" Click on the > button to display additional BITs, or Bloomberg Intelligence Themes.

JON ASMUNDSSON