THE BLOCKCHAIN
IDENTITY

CAMPBELL R. HARVEY
Professor of finance at Duke University

2017 CFA Institute Annual Conference
Philadelphia, Pennsylvania
23 May 2017

This session from the 2017 CFA Institute Annual Conference covers:
• What is blockchain technology, and how does it work? What are its benefits and
  risks, who will be disrupted, and who will be the disruptors? Is this technology just
  hype or is it real?
• How might the distributed ledger of blockchain improve upon existing transaction
  and ownership protocols? What stands in the way of large-scale adoption?
• What are the practical implications of blockchain in the near and intermediate terms?
  Should today’s financial professionals allocate time and resources to blockchain
  technology or pursue a “wait and see” strategy until there is a clearer path for this
  complex technology?

CAMPBELL R. HARVEY: So, I’m not going to talk about the misrepresentation of earnings,
OK? Though I could. I’m going to talk about something that is kind of different from my usual
research. And it has to do with a blockchain. So to be perfectly honest, this is the first hour of
the course that I teach at Duke University to second-year MBA students, and the course is called
“Innovation and Cryptoventures.” I’ve taught this course for three years. I just finished teaching it.
It’s a fairly popular course. And maybe you’ll see why.

I’m going to focus on the technology as well as applications. My course is not really a finance course.
And you’re going to see that many of the applications of this technology are not in finance, OK?

My goal today is to try to communicate the basic idea of blockchain. So, you’ll have a basic under-
standing of what it is, and we’re going to introduce some concepts that you might not have heard
of, like cryptographic hashing. And I go into some detail. You might not like that detail, but we’re
going to go into that detail.
So you will be, after today, hopefully in the 0.1% in terms of your knowledge of blockchain technology. And I think this setting at the CFA Institute conference is a great setting for this. And what you need to be thinking about is that you want to be the disruptors, not the disruptees. OK? And blockchain is a highly disruptive technology. So, let me go through and give you a sketch of what’s actually happening here.

First thing, blockchain is the technology. There is no “the blockchain.” There’s many different ways to actually implement a blockchain. And indeed, the idea of blockchain is not a new idea. It’s from 1991. There’s a paper by two researchers in computer science that actually details this technology. And the application was time stamping of documents in a secure way. And we’re actually going to see that this application, the original application, has got a fair bit of relevance in terms of what we’re going to do today.

The other thing that’s a huge misperception, and that is many people believe that Bitcoin is blockchain. And indeed, this is perpetuated in the press where they interchangeably talk about blockchain and Bitcoin. Bitcoin uses blockchain technology. There’s many other applications that use blockchain technology. We will talk in some detail about Bitcoin today because it is an important innovation, and there are many other cryptocurrencies that are out there also.

OK. So what is blockchain? So, blockchain is a ledger. It’s almost literally like a spreadsheet. And what it does is it’s a ledger that’s shared. So, it’s distributed, and indeed, these are three diagrams from a very famous paper in 1964 that was one of the foundational papers for the internet. And the motivation was a Soviet nuclear strike on the US, wiping out the main computing systems. And if the computing system was centralized, a hit on the central location would take out the nation’s computers.

So, they started exploring decentralized and distributed. And the internet is kind of a combination of decentralized and distributed. You can take a piece out, but you can’t take the whole thing out. So, blockchain is going to be distributed. It’s a ledger that, essentially, depending on the application, anybody can download — have it on your computer — a copy of this ledger. So, blockchain also can be transparent or have varying degrees of transparency. And I’ll talk about that a little later on.

The number three property is that it’s immutable. And this is very important. So you can add to a blockchain, but the idea is that you cannot go back and rewrite history. So, you cannot edit. So, this is where it’s different than an Excel spreadsheet. So Excel spreadsheet, you just go, and you can edit some entries. So, with this technology, once it’s there, it’s there forever. OK? So, if there’s a mistake that’s made, maybe you can undo the mistake with another transaction. But you can’t go back and change anything in the history. So, this is a big innovation and important, as we will see fairly soon. OK.
And the fourth property is that this ledger is cryptographically secured. So, I've got a little diagram at the bottom. I'm going to go through more detail about this diagram, but essentially, what's happening here is there is a commonality in these blocks of transactions. So, it's called blockchain because transactions are lumped into blocks, but there's a commonality in that the very last line of one block is the first line of the next block. So, that's the link, that's the chain in this particular structure.

So again, this is different than an Excel sheet where there's nothing like this. It's just one sheet. You could have subsheets, but they're not linked like this. So this is basically what a blockchain actually is. So, for technology to be disruptive and successful, it has to solve problems, and this definitely solves problems. OK. So, we can use the blockchain, or blockchain technology, to basically do two general classes of operations. Number one, we can verify ownership very quickly, very efficiently that somebody actually owns something. And number two, it allows for the efficient exchange of ownership on this blockchain.

OK. So, one person that's a loser is the middle person. So, any situation where you've got a lot of middle people, this is probably a situation where blockchain could be very important. So, everybody is treated the same. So, we usually think of a customer, a retailer, a banker.... No, everybody is treated equally in this technology. So again, this is the general overview. I'm going to go into much more detail and many more applications. But let me just start by motivating a few kind of obvious applications of this technology.

So, this is a shot of the NYSE from the 1920s. In the 1920s, it took five days to settle a stock transaction. In 1995, a revolutionary change happened where we moved from so-called t + 5 to t + 3. This was in 1995. Today, we're t + 3.

And if you think about this, 1995 — that's the beginning of the World Wide Web. Internet becomes very accessible; popular computing speed is dramatically increased. Yet, we're still stuck in t + 3 to settle a stock transaction. That, to me, doesn't make any sense.

And indeed, the clearing corporations understand this. This should not happen in three days. This should happen in a matter of minutes, and blockchain is exactly the technology that can do this. OK. Second application — property. And for those of you that have bought a house, you know what you have to do. It is a relic of history. You have to do a title search — you have to employ lawyers often to do that. And the reason for the title search is that you want to make sure you're buying the house from somebody that actually owns it.

OK. So, we have to go through this process to actually.... and if you get a mortgage, you might have to get title insurance because the bank doesn't want to loan you the money to buy a house from somebody that might not even own it. OK, so this is a nightmare.
So again, blockchain technology is ideal for this. You have every municipality putting every single piece of land into a blockchain — every single piece. And then anybody can download it. You go into your realtor’s office or your lawyer’s office, you see who owns the land, you see the liens on the land — the mortgages and stuff like that — and you can instantly do the transaction, very low cost. OK. So, this is an application of verification so you can verify that somebody actually owns the property. It’s also an application of efficient exchange. And something that we should have, that we don’t have.

Transferring funds — this is one of the low-hanging fruits of blockchain technology. We constantly hear that SWIFT, the messaging system that enables wire transfers, is under attack. And it has been hacked multiple times, OK? And recently the New York Fed and a Bangladeshi bank got taken in terms of a SWIFT fraud. So, chain enables the transferring of funds in a highly secure way. I need to prove to you that it’s highly secure, but that’s going to be fairly easy for me to do.

So, this is just another application and a very important application. So again, the general idea of money transfer — today, it’s very inefficient, very insecure, the fees are high, and often the fees are high to pay for the fraud detection. So if you can introduce a technology that actually is secure, you don’t need to invest in the fraud detection.

So what about counterfeiting? That’s the most counterfeited bill in the world. And there’s the prime perpetrator of the counterfeiting. So, it’s kind of obvious that we will go to digital currency. It’s kind of obvious. But there’s a problem, and it’s the same problem that we have with copying digital music — you can make a perfect copy. Digital video — a perfect copy; a picture — a perfect copy. Well, a simple version of digital currency — and people have been trying to do this since 1981… that was the first digital currency that was introduced. Every single one failed. And the problem is that it’s so easy to counterfeit. You can make a perfect digital copy.

Blockchain solves the problem. So, think of blockchain very roughly, at this point, of taking seriously the serial number on a bill. So, that’s effectively what we’re going to do, and all of the major central banks are looking into digital currency, and every single one knows that it’s got to be based upon blockchain. OK? So, that is part of it.

OK. Here’s another application of verification. So, you get into your car, you put your thumb on your phone, and a blockchain is checked to see if you actually own the car. If you own the car, the car starts. So, that’s a verification of ownership.

But the blockchain can be a little more complicated than that. So, the blockchain could actually have a condition. So, maybe you have a loan on your car. And in the loan contract, it says that if you miss three monthly payments in a row, you’re in default. And suppose you’ve missed three monthly payments in a row. You go into your car, thumb on the phone, it checks the blockchain, the car doesn’t start. The car starts for the bank. This is the sort of stuff that’s possible with this technology.
So, as I said, any situation, any situation where there’s middle people, in general, peer-to-peer technology will be disruptive. So again, think about situations where there’s a lot of middle men. I recently did a conference in — it was actually sponsored by the law school — on digital music. And the number of middle people involved is so extreme that the artist, even well-known artists, are lucky to get $0.25 on a dollar of revenue. That is just prime area for disruption with this technology.

OK. So, I’m going to talk about two different types of blockchains. So, in very general groupings, there is a public blockchain, and there’s going to be private blockchain. It’s important to understand both, though most of the kind of business applications these days are focused on the private side. But I want you to understand the public blockchain.

And the public blockchain is basically structured so you don’t need to trust anybody. So, people refer to this as a trustless technology. And I’ll talk about the Bitcoin blockchain because it is the most secure blockchain right now in the world. This is a computer program. It’s open source, so indeed, you can grab the computer program that’s available to anybody and make a minor change and create your own coin. I did this. I created Camcoin. It’s not very popular, but it’s really easy to do. So, anybody can do this. And within the public domain, there are many choices that you make in terms of the blockchain technology.

So one of…. The second most important cryptocurrency is called Ethereum. And Ethereum has got this advantage that you can actually do contracting within their blockchain. So, you can have an “if/then” condition. So, if IBM stock finishes above $100, then I get a certain payoff — so, like an option. So, any if/then statement can be embedded in their blockchain.

The Bitcoin blockchain is more rigid. But again, it is the original one from 2009. There are various mechanisms that are used to validate and to secure these blockchains. And I will talk mainly about something that’s known as “proof of work.” And I need to describe to you what that work is.

A private blockchain is a situation where you actually need to trust somebody. So, it might be that the municipality sets up a private blockchain and puts all the land in. You actually need to trust the municipality to put those entries in correctly. Or it might be a consortium of banks that get together and allow for more efficient transfers between the banks. And again, you would need to trust that group of banks. So, it’s very important to determine, when you’re thinking about the type of blockchain, to determine how important it is to be trustless, or is it OK to allow for some trust. Trustless actually has a cost to it, and I’ll describe that cost in a few minutes.

So, I’m glad you’re here because I really do think that everybody should understand the cover story in The Economist. So, that should be part of the CFA® designation, that at minimum, we should understand what is going on with blockchain. And this is not a small thing. So, I talked about clearing, and the DTCC is looking at blockchain technology to clear derivatives. That’s an $11 trillion market. So, you can see that there’s big upside with this particular technology.
This is just recently. Spotify buys a tiny startup called Mediachain, and again, they recognized that within the digital music industry there are many problems that blockchain can actually solve. OK. So, let me talk about the Bitcoin blockchain. So, it is distributed, it is secure, it is transparent. So, that means anybody can download this and see the plain text transactions. And every single transaction is in this blockchain. The blockchain is about 95 gigabytes. So, it’s not really even that big.

So, anybody can download it, and it establishes ownership, allows for efficient transaction at very low fees. OK. Nobody controls it. It is trustfulness. So there’s no CEO of Bitcoin. It is a computer program. And in my course, we talk about DAOs. And DAO is not the Dow Jones average. It’s a distributed autonomous organization.

This is a computer program that has created a lot of value. And literally, people work for the program. So, people are actually working for a computer program. It is a glimpse of the future. So, this particular blockchain is actually secured by unprecedented computing power, and I will go into some of the strong cryptography that’s used so that it cannot feasibly be hacked.

So, I’ll talk a little bit about miners also. They’re the ones that verify and provide the security of this particular ledger. So, how powerful? And this is really, to me, staggering. The Bitcoin network right now has the equivalent computing power of 47 million petaFLOPS. So, “FLOPS” is floating point operations per second. Compare that to the fastest supercomputer: It’s 93. So, 47 million compared to 93.

So if you’re in the know about this technology, one thing — and this is important — you actually don’t need to do floating point operations. So, the sort of technology that’s used for the Bitcoin blockchain is more akin to a GPU rather than a CPU. Nevertheless, to actually cause any problems with this blockchain, you would need half of the computing power of the network, and it’s going to cost well over a $1 billion to actually do that.

So, all of the average hackers, they cannot touch this. Maybe a state actor, a nefarious state actor could disrupt the current transactions, but it is extremely unlikely that they can go back and rewrite history. So, this is unprecedented computing power that is behind this particular blockchain.

OK, so the first term that might be new to some of you is “hash.” Not hashtag, but cryptographic hash. So, I’m going to do two examples. One is a very simple one that points out the problem with this particular simple hash, and then I’ll do a more complicated one where I’ll go to the internet.

So, let’s say I want to send an email to Marie, and I’m worried that that email is going to be intercepted and corrupted. So, what I’m going to do is to do a simple hash of the single word in the email, “hello.” And my simple hash is I will assign a number to every letter. So, A is 1 and Z is 26.
So, when they do that, it’s 8-5-12-12-15. And my hash is going to multiply those numbers together. And I get 86,400. I’m going to post that hash on my website.

I’ll send the email to Marie, Marie takes the content of the email, applies the same hash, and gets 86,400. She checks my website, she sees the 86,400 — therefore, she’s confident that the message has not been corrupted.

So, notice that if the message was corrupted — and I’ve got an example here of “hallo,” rather than the “hello” — you get a different number. And you can detect the corruption with this hash. So, this hash is too simple to work in a serious context like cryptocurrency. And the reason is that if you mix the order of the letters around you get the same hash.

So I’ll give the example of changing “hello” into “ohell,” which has a different meaning but the same hash. OK. So, the second kind of new term here, which is a term you know, but in this context it’s called a collision. So, a collision is where you have two different inputs, hello and ohell, that delivered the same hash. You want to avoid that.

So, we need to do something more complicated. And this is going to be the so-called SHA-256. So, that’s the third term I want you to remember from today — SHA-256. That’s secure hashing algorithm, invented by the NSA. You might be a little suspicious, given, for good reason, for the NSA, but this is open-source code. It’s been checked by many people. There’s no back doors or anything like that; it’s all very straightforward. And what we do is to take an arbitrary input, which could be an email or it could be a transaction, put it through this function — and this is, as I say, a cryptographic hash — and it delivers 256 bits, zeros and ones.

So, to be clear, this is not encryption. This is hashing, it’s cryptographic hashing. Encryption is where you take a document, encrypt it, and then there’s a key to decrypt it. This is a one-way function. So, I could take something that is one word, and it turns into 256 bits. I could take something that’s 10 gigabytes — it turns into 256 bits. So, we’re not going to be able to reverse the hash. OK? So, this is not encryption, it is hashing. So, what I’d like to do is to go to the internet and actually do some hashes to show you what this actually looks like.

So, I’ve typed in “hello, world.” And let me calculate the hash that’s associated with this. And hopefully you can see this at the back. It is basically a code that is not zeros and ones. It’s in hexadecimal.

So, hexadecimal is zero to nine plus the first six letters of the alphabet. OK, so that’s unique. OK, so this is the 256 bits. And if I go and change this very slightly, so let’s say I put a 0. So, notice the hash is 315F5. It starts with that. So, let’s say I put a 0, and I recalculate the hash. It’s completely different — 312AF, completely different.
And if I go and go back to the original and rehash, I get back to the 315F. OK, so this is the SHA-256. And let me just do one more here that I'm going to use a little later on. Let's say I put a number 4-2-5-0 afterwards and then hash. And notice that hash is a little unusual in that it's got four zeros at the beginning.

The probability of any zero or any letter is 1 over 16. So, the probability of getting four zeros is 1 over 16 times 1 over 16 times 1 over 16 times 1 over 16. So, that's rare to actually get that. So, this rare hash is going to be important.

So, let me go back to my PowerPoint presentation and show you some more examples. So, the first one is a hash of the King James Bible. OK. So, I found it on the internet, just copied it into the same program, hit the hash button — instantly I get that hash. And then, the second one is the Bible with the last word omitted — “amen.” — it's gone. Notice, it's completely different.

And indeed, you can do a hash of a hash, and that's what I did for the very last line. This stuff is crucial for any blockchain technology. But this is a general idea. Indeed, we can think of this in many different dimensions. I will talk about an application to email. I'll talk about the application to Bitcoin.

People ask me a lot, can we undo the hash? Intuitively, it doesn't make any sense that you can undo a hash because, as I said, if you've got 256 zeros and ones, how can you feasibly invert that to get the Bible back? It just doesn't make any sense.

But technically, you could do this. And it's by brute force, and you need to guess 2 to the power of 255 different combinations. And when I say infeasible, I really mean it. Because to do that is... basically, the number of trials you have to do is equal to the number of atoms in the known universe. OK, so it's just infeasible — so very, very secure.

OK, so let me return to the email example. So, now I'm going to send an email to Marie. I want to make sure it's secure. I take a hash of the document — maybe it's not just a word, but it's a document that I'm sending — I take a hash of that document, I post it on my website. Marie gets the document, drags it into the same program I showed you, gets the identical hash that I've got on my website. I am confident. The probability of collision is very, very low with a SHA-256.

OK, so this is a secure way to actually validate. So, this happens, actually, all the time. So you don't even know it's happening. This happens when you send an email. So, I challenge you to go to your email program, whether it's Gmail or Outlook, go and look at properties, view the header of the email, and you're going to see references to SHA-256, SHA-384 — which is a longer one — 384 bits. OK? It's going to be there. It's used routinely to guarantee that files are not corrupted.
OK, so I can’t resist showing this one. During the election, WikiLeaks was interfering with the electoral process and releasing Podesta’s emails and things like that. At some point, the internet was cut off at the Ecuadorian embassy in London. And when that happened, three Tweets were sent out. And this is the story from the *Wall Street Journal*. It just so happened that was the same day that Pamela Anderson “visited” Julian.

And the *Wall Street Journal* basically says each one, and I’m showing one of them, began precommitment and then the number 1, 2, or 3 — so there’s three of them — followed by a short phrase and then an assortment of 64 letters and numbers. OK, those 64 letters and numbers are a SHA-256 hash.

So, you know that now. The reporter at the *Wall Street Journal* didn’t know that. So, this is not just any assortment; this is a hash. And the story missed the main point.

So, why would this… why would WikiLeaks say John Kerry, precommitment number one, and then deliver a hash? So, it’s clear to me what the story is. And the story is that this hash proves that WikiLeaks has a document that’s very sensitive for John Kerry.

So, John Kerry… actually within the government…. The government keeps hashes of all their documents, so it’s very easy for them to do a search for this hash. And with this hash, it is proof that they actually have access to, potentially, a highly embarrassing document. So again, there’s many different uses for these hashes. And blockchain is going to use this in basically private and public implementations.

OK. So as I said, everything on the Bitcoin blockchain is public. And this is the same diagram I showed you before, where now the code that is linking the blocks is a SHA-256. So, these are just plain text transactions. And at the bottom there’s a SHA-256 that reappears at the top. That’s the link. So, the SHA-256 is the linking mechanisms.

And let me show you a simplified example. So, this is with shorter hashes, but you kind of get the idea. So, you can see all the transactions. You can see the people that are transacting. And notice the way it works, we’ve got a block 99. And there’s a hash of that block that appears at the first of the next block. And then this is hashed. And it appears at the beginning of block 1,001.

So, within block 1,000, I actually buy a car from John. So, you can see that I’m docked 17 Bitcoin. And John gets 17.

So now, suppose I go in and edit that block. And I change, very subtly… all I’m going to do is to flip the plus and the minus. OK, so now, I buy a car from John, but he pays me the 17. It’s a great deal.
OK, so I made a very subtle change. I’ve just switched the minus and the plus sign. But the implication is pretty severe because when that block is hashed, it delivers a different hash than the beginning of block 1,001. So immediately, the algorithm says this block is not valid. It goes out to the network and gets the correct block.

So, this is a way to ensure integrity. This is a way that we can prevent the rewriting of history and any credible hacking of the blockchain. So, it’s a little more complicated than what I’ve described. So, it’s not just a plain old hash like I did on the computer. It’s a special hash. So, we take the transactions and then we add a number, a magic number, and it’s called a *nonce*. N-O-N-C-E, that’s the fourth word that might be different for you today. So, we’re going to add a number. And what we’re going to try to do is to get a special hash that’s got a lot of leading zeros. That’s the idea.

And I did one for you where I put 4-2-5-0 and got four leading zeros. So, it’s going to be difficult to get these leading zeros, and this is why we need the massive computing power. So, this is very important for security. And think of what we’re doing — another way to think about this is you’ve got five decks of cards, you shuffle them, and you try to… the first five cards are aces of spades — very unlikely. So, you’re going to have to do a lot of shuffling, and for what we’re doing, we’re going to have to do a lot of hashing to try to get these leading zeros.

And that’s exactly what happens — a huge amount of hashing. So, the current blockchain has 18 leading zeros. It is very improbable to actually find that winning hash. Indeed, the probability is about the same as winning the Powerball twice, like in a row. OK, so there’s a massive amount of power that’s actually behind this.

And interestingly, the algorithm is immune to increases in computing power. So, what it does is it targets a winning hash probabilistically every 10 minutes. If the hashes become found like, let’s say, every 5 minutes, then automatically the difficulty is increased. So, instead of 18 zeros, maybe you go to 19 zeros. So, it’s automatically adjusting so that the transaction blocks are done every 10 minutes.

So, this is approximately how this works. And the miners are actually the ones that are doing the hashing. And they are in a contest. And whoever wins or finds a hash with 18 leading zeros — people go, it’s posted, and it’s very easy to verify. So, anybody can verify — I can verify it here with the program I just showed you.

I just copy the transactions and the nonce that they use. And maybe it’s like 2,435,016. Put that in. Run it through my program. I get the 18 zeros. It is verified. So, the miners are verifying the transactions, verifying that people actually have the cryptocurrency to spend. And then the miners are also securing these blocks. You might wonder why. Why do we need 18 zeros? Why do we need all of this computing power to actually secure this network? And the reason is that we don’t want people to go back and easily redo, block-by-block, the history of the blockchain. With 18 leading zeros or 17 leading zeros, it’s just not feasible for anybody to actually go and do damage to
the history. So, that’s the reason it’s there. It’s trustless. We don’t need to trust anybody here. But it is cryptographically secure.

OK. So, this is also, I guess, important for other blockchains. So, I mentioned the Ethereum earlier. Ethereum blockchain actually is the same concept, where there’s hashing going on. They will actually switch their protocol in the future to a consensus mechanism called proof of stake. I’m not going to go into that today, but it is a topic of what I do in my course.

Also, I should mention that my course, all of my materials, are online. So, it’s on my website. All of my PowerPoint decks, all of my lectures — everything is online. So, if you’re interested in going a little deeper, this is available.

OK, so let me talk about private briefly before I get to some applications. So again, private is where you trust people. And one example that I gave earlier is the banks. The banks are working with legacy computing. Indeed, the most valuable coder today is one that knows COBOL, a language of the past, right? At least 35 years old. When I was an undergrad, they were using COBOL. But even then, it was being replaced by other languages.

So, it is a legacy infrastructure. Banks spend $200 billion a year maintaining the legacy architecture. What could blockchain potentially do? And check this out. This is a simple example: three banks — A, B, and C — and two customers. Banks do business with each other. Customers do business with potentially more than one bank.

And this is a simple network diagram. And it’s really simple, three banks, two customers. Can you imagine a billion customers and 100,000 banks? So, this is really simple. Everybody’s got their own ledger. What can blockchain do? And this is what it can do. On the right is a simple ledger where everything is shared. OK, so very easy to deal with. And actually it’s also interesting, my interaction with regulators. Initially, regulators were very negative on blockchain because they thought blockchain meant Bitcoin. And Bitcoin associated with Silk Road, and ransomware, and stuff like that.

When you showed the regulator this diagram, you can see the glitter in their eye. One place to look — so they get access to, basically, all of the bank’s records in one place. So, this is so simple. And all of the banks are working on some sort of blockchain technology. It might not look exactly like this, but you get the idea that this is a way to do away with the legacy architecture.

It’ll take a while to do, but some banks actually have this operational. And I point you to JP Morgan’s Quorum, which is a very interesting technology. And one thing you might think immediately, well, what? One ledger, I shouldn’t be able to see my competitor’s transactions in this ledger. And Quorum actually solves this problem.
So, everything is in a blockchain. But you only get to see the transactions that you are party to. OK, so it’s a great idea. It is operational. It’s not just an idea. It is operational. And it is also open source, OK, so it’s available. So, very exciting.

So let me, before I go to my main applications, talk about an obvious application of blockchain. And this has to do with machine-to-machine transactions and payments. So, I see the internet in three different phases. One, the first phase, was just gathering information. You go to a new site, and you get the information. Or you go to Wikipedia, you get the information. The second phase of the internet was social, so social media, Facebook, Twitter, Instagram, stuff like that. The third phase we haven’t seen yet, but it’s coming. And this is, basically, enabling machine-to-machine payments.

So, if you think today, it is very clunky to do payments on the internet. So you have to put credit card information in. And who knows how secure that is? Sometimes you even put bank account information in. And again, that’s even more dangerous in terms of security.

And notice that we’re doing the paying. We’re not getting paid. There’s no way currently, in a simple way, to actually be paid. There are things like PayPal, but the fees involved are significant. Credit card fees are very large, 3% — you swipe at a gas station 7%. OK, so this is all because of the insecurity of these particular mechanisms. So basically, there’s no mechanism for me to charge for something. So, you download one of my research papers. I spent a long time working on that. I can’t monetize it. Even if I got 5 cents, that would help. But no. So, nobody is going to do a credit card for 5 cents.

So, what can we do here? And the key is HTTP 402. And you know 404. Everybody’s got a 404 error — website not found. So, look up 402; 402 is built into HTTP. And it is for…. it is for digital micropayments, except there’s no ability to do that in the past. We have the ability to do that today. And one company that’s heavily into this is called 21.co. You should look them up. So, their idea is to enable this HTTP 402.

So in terms of payments, I said that it’s hard to be paid. Well, actually, you can be paid for doing tasks. Amazon Turk is the leader in this., but it only works in the US and in India. And the payments you get are once a month. With this technology, the payments could be instant.

So, think about — and I tell this to my students — you’ll hop into an Uber. You do a couple of surveys or tasks on your smartphone. You’re paid $2.50 for each task. That’s enough to pay for the Uber.

So again, this is like a machine-to-machine payment, instant basic pay for doing a task. So, another way to think about this is changing your view of email. So, think of email where, at the top of your inbox, you’ve got friends, family, your work stuff. But there’s many other people that want to get to the top of your inbox. Well, they’re going to have to pay for it. So, you set the price. You set the price to get to the top of your inbox. And when they send it, it instantly goes into your
account. Let’s say $10. And if you open the email, you get paid. And if you go to a website link, you get paid. This is a completely different model, and it’s a model that basically makes email expensive, but not that expensive. So, you have a price that’s set extremely low, 1/10 of a cent, let’s say. And that means anybody in the world won’t be prevented from using email, but what it will do is to eliminate spam. Currently 66% of the email that comes into my university, duke.edu, never goes to any inbox. OK, it is just pure spam — 66%. So again, you put these people out of business with this technology.

And we can extend this to the web — so make the World Wide Web no longer free. Again, you have the very, very small price that people can pay. But again, it puts the people doing distributed denial of service attacks out of business. They cannot afford to do it. OK, and again, we free up bandwidth. It also allows people to monetize their content. And this is a big deal today, actually, especially in media. It’s very hard to monetize. Even the leader in paywall, New York Times — 90% of the traffic that comes to the New York Times site are not subscribers. So, with a small fee, it allows media sites to actually generate some extra revenue, where maybe they can employ some fact checkers and editors. So, all of these are possible with this technology that is enabled with blockchain.

I am very negative on Facebook and Google. Because… so currently, 80% of online advertising is basically with Google and Facebook. And the example on the side is Google AdWords. And this is, I think, not sustainable.

So, you do a search for “Dallas truck accident lawyer.” And you go to a particular website of that lawyer that is basically number one on the Google search. That lawyer pays Google $425. You get nothing. That’s not sustainable. That’s going to go away. Google is a little more diversified in their business. But Facebook isn’t. So, this is a short-term thing that will go away. And this idea of micropayments hits so many different industries.

Think of cellular companies — AT&T, Verizon. This is going to be completely different. People will own the towers. You use the tower, you pay a small amount, 1 cent, 2 cents. You pay to directly to the owners of the tower. OK, these large companies are effectively middle people. And blockchain allows the disruption of the middle people.

So, it’s not just this. It’s cloud computing as we know it today will not exist in the future. Computing in general, it is a wasted resource. The average desktop computer uses only a couple of minutes of full CPU a day. And that can be harnessed to basically do cloud computing, OK? But a different version, a distributed computing. OK, so this is a big deal in my opinion.

Let me talk about a few applications before we go to questions. This is a ballot for Brexit. And Brexit would never have happened if there was blockchain voting. And it turns out that the younger people were very remain, like stay. But they did not vote. And they didn’t vote because, oh, why should I spend hours going to the polling booth, standing in line, and doing this archaic
check on a paper ballot? Why can’t I do that on my smartphone? Well, blockchain allows you to
do it on your smartphone. So, we're going to see applications with voting. It’s a low-hanging fruit.
It’s also secure. You get instant results. There’s no hanging chads. It is clear and secure.

The internet of things — so some of the main blockchain applications are internet of things. This
is my Nest, a picture of my Nest. I actually don’t think it’s a good idea that somebody can hack
into my Nest and set the temperature to 110 degrees. OK, so again, I want this so that only I can
actually do the changes. And again, think of a lookup to a blockchain. Yes, this is my Nest. I can
do a change.

So, if you think a Nest is one problem, think of it — a self-driving car. Like, I definitely don’t
want to get into a car like this and have somebody take it over. OK, this is very dangerous. So to
me, blockchain has to be part of self-driving cars. OK, you do not want to take the risk of some-
body hacking and taking control of your car when you’re in it.

This is an obvious application. It is a scandal today, what happens, especially with opiates in the
US. These scripts are still used. People go into the office, they steal the script, they go fill multiple
prescriptions. Again, this is such a simple application, where there is a prescription blockchain.
Everybody’s got it. The doctor, effectively, gives you a token for a particular drug.

You can go to any drugstore to get it filled. You can’t sell it. And it expires. And it could be used
only once. And it’s in the blockchain. So you go into the pharmacy. The pharmacy looks up and
says, yes, you’ve got this token to spend on this drug. And it’s done. So, this is a very straightfor-
ward application that solves a huge number of problems in terms of the social issues and the health
issues induced by drug abuse.

Medical records — no problem. We’ve got a blockchain application for it. So really, what we’re
talking is, a large hospital might have two million patient records protected by a single password.
That is just unsatisfactory. So, with blockchain, you take control of your own record; you’ve got,
effectively, a key or a password for your record.

So, if somebody hacks into the two million patient data, they’re going to have to crack two million
passwords. That’s very unlikely. So, this solves an important privacy problem. And it solves the
issue of you going to a different provider and them not being able to access your records.

Well, they can access your records now. You give them permission. You are the owner of your data.

Financial statements are a relic of the past — annual statements, quarterly statements. An obvious
blockchain application is for a company to use blockchain technology for, basically, their account-
ing. And then there’s an API that delivers the same sort of information that you would usually see
in a quarterly statement but in real time.
And when you do that — and there is actually a link to my paper here that won the Scroll — you eliminate all these shenanigans that are happening at the end of the quarter or end of the year because everything’s real time. And in real time, people realize that there’s some noise. OK, so this is an application — I actually think the main accounting firms are in a good place. I said I was negative on Facebook, but I’m positive on the accounting firms because they will still be used to validate transactions, not just financial transactions, but all types of transactions.

So, I buy the Nest. And there’s a blockchain for Nest. They will validate that I actually own the Nest. So, there’s a good business path for them in the future.

Property I already talked about. Digital twin is a very hot application of blockchain. And this is the idea that every single part, every single sensor reading, is put into a blockchain. So, then when you actually — if there’s a problem with the jet engine, you actually look and you see that a part that was put in was not the part that was put in on the blockchain. That’s fraud. And the trial is very swift. You’ve got the blockchain. It is telling the truth of history.

It’s also the case that it’s easy to resell the engine because you’re handed the complete record that cannot be doctored with. OK, so you get rid of the so-called lemons problem, that you don’t know what the quality of the engine is. Well, you’ve got all of the details. And this is just one example of a digital twin. It could be many other examples like this.

Fedcoin — so I mentioned all the central banks are looking at blockchain. And it is remarkable to me that 78% of the value of US dollars today are in $100 bills — 78%. Yeah, think about that. You go to a store. It says we do not accept $100 bills, or $50 sometimes. Yet 78% is in $100 bills.

So why? And it’s pretty clear, there’s the stash of El Chapo. OK, so he’s got a pile of $100s. And the two smaller stacks are two things, 10,000 yens and 500 euro notes. So this is a big problem. Again, blockchain can solve this problem. And it will likely be called Fedcoin or something like that. All of the central banks are pursuing blockchain applications.

The Bank of England is maybe the one that’s out ahead of everybody. And notice the paper that they put out. And it’s very interesting. Look at the icons. So, you see the diamond? You see what? Diamonds and blockchain?

Well basically, the issue is the blood diamonds. So you want to be sure that the diamond actually is not a blood diamond. So, you actually laser in a code in the diamond. And you put that code in a blockchain, and it essentially verifies that the diamond is clean.

In the Middle East, see a passport. On the side, you see a power. So, people are using this for energy trading. IBM’s got a contract to put the US power grid on blockchain. There are smaller
applications, where people with solar panels are sharing their power on a peer-to-peer basis. There’s no middle person. OK, so many applications here, including the cryptocurrency.

OK, so let me finish. This is... in my course, we do the technical details, but we also do innovation projects. And in my course, it’s kind of high-stress because 100% of the grade is on a 15-page pitch deck of a new company based upon blockchain technology. OK, it’s high stress.

And these are some of them. I won’t go through all of them. But let me just mention number one — smart guns. So, it was in the press recently. Can you imagine a gun, where it’s activated with your thumbprint just like your iPhone? So only you can fire the gun.

But think about the application for law enforcement. So, the smart gun again, is activated with the thumb. But it’s also got GPS. It also can keep track of every single bullet fired. After the day, you put the gun in the rack. And whatever happened to that gun goes into a blockchain. And this basically eliminates a lot of the uncertainty as to what happened. We know exactly when the bullets were fired. And we know the direction, and the angle, and the person that’s pulling the trigger.

OK, so this is a very simple application. And maybe it’s not a lot of money in this application. But it solves a problem. And I think it is promising. So, there’s many different ideas, and I’m always amazed. This is the third time I’ve taught the course, and I thought that the projects would just repeat the projects of the previous year. And I had student groups coming into my office proposing... we can’t decide upon three ideas. And each one of the three would be different than the year before.

So, the message here is that this technology is not going to go away. Bitcoin and Ethereum might go away. But that’s just one application of blockchain technology. We’ve seen some of the low-hanging fruit in terms of financial applications, but there’s plenty of applications outside of finance. So any time, as I said, that security is important, where we need to verify ownership of any property, and if middle people are involved, this peer-to-peer technology can be very useful.

So, I will end it there. And I see we’ve got lots of questions.

ELAINE CHENG: There are a few questions.

CAMPBELL R. HARVEY: OK, good.

ELAINE CHENG: Let’s give Cam a hand for that, and we’ll move on to questions.

[APPLAUSE]

OK. Yeah. We have a lot of questions here, so we’ll try to get through as many of them as we can. You talked a lot about the security of blockchain and how that security works. I think we have a
couple of doubters still in the audience. I think they’re just curious: Under what scenario would the blockchain be at risk from a hacking situation or a compromised situation? Maybe you can just talk to that a little bit.

CAMPBELL R. HARVEY: Yeah. So the main risk would be that — you have to talk about it in two different ways. Number one, if it’s a private blockchain, then it is potentially at risk. So, think of, let’s say, 20 banks getting together, and then somehow somebody takes over the computers in 11 out of the 20 banks, they could cause some havoc in that private blockchain. I think it’s unlikely that somebody could simultaneously take over the banks’ computers for 11 of the 20, but nevertheless, that’s a possibility.

On a public blockchain like Bitcoin it is solid, right? So, the cryptographic hashing that’s necessary to actually go and start changing history — it’s just infeasible to think about rewriting history. But there could be other public blockchains that don’t have as much power behind them that could be susceptible to a nefarious actor coming in and disrupting. So, nothing is perfect. And I chose my words very carefully. I said it’s infeasible to hack. It’s infeasible to undo a SHA-256, but it’s not impossible. So, it is possible, it’s just very unlikely.

ELAINE CHENG: Thanks. Just a little bit of a follow-up question… and there were some questions in here about, in the news, hearing about hacking of a Bitcoin. Maybe just addressing that and —

CAMPBELL R. HARVEY: Sure. So, Bitcoin was in the news, I guess, for many negative reasons. So, Silk Road, for example, where you buy drugs with Bitcoin — and it was closed down. And a lot of criminals tend to use Bitcoin, but they haven’t had the luxury of sitting at this conference and actually hearing my presentation. Because the complete record of whatever they do is in a blockchain. A criminal definitely doesn’t want that. So, you can do the initial transaction, so you pay $300 in ransomware. It goes to an address that’s well known. As soon as the criminal starts to spend that, we can probabilistically figure out who it is.

So, don’t think that Bitcoin is anonymous. It’s more anonymous than, let’s say, a credit card. But it’s not anonymous. Indeed, I would say that blockchain is the last mechanism for an illegal transaction that you would want. OK, again, as I said, the court case is very short. Here’s the record. It’s immutable. This is you? Uh, guilty. OK, so it’s that’s the last thing you want to use.

And what I recommend — well, it’s actually weird to recommend things for illegal transactions — but cash. So, cash is what you should use. It’s a big mistake. And WannaCry is in the news all the time about this ransomware that encrypts your data on your computer. There are three Bitcoin addresses that are given. People are watching that so carefully, I doubt that the money that they get will ever be spent, OK? Because as soon as they start spending, they’re in trouble. OK, it’s the same thing with Silk Road.
So, the other thing in the news was the so-called hack of Mt. Gox and an enormous amount of Bitcoin that were stolen. And people think that that is a hacking of the blockchain. It has nothing to do with the blockchain. It has to do with a third party that is acting as a bank. So keeping your codes in this bank — and in the press, I’ve referred to this Mt. Gox as a bank. And think of a bank branch that has no security cameras, no employees. The doors are open. The vault is open. And you just walk in and take the codes. That’s the level of security. Mt. Gox, it stands for Magic: The Gathering Online Exchange — so a trading card exchange that happened to get lucky with Bitcoin. And people knew that they were not secure, and people kept their Bitcoin there, and the Bitcoin got stolen. OK, so this is a third party, and a very low-quality third party. With a new technology, you’re going to get situations like this.

In contrast, Coinbase, which is a Bitcoin and Ethereum bank — you put a deposit with them, it is insured up to 99.8% of the value by Lloyd’s of London. So, if Lloyd’s fails, that’s another issue, but nevertheless, very, very secure. So, we see stuff like this. But for Bitcoin and for the cryptocurrency, it’s not really an issue. There’s no hacking. You can hack the third parties. But the blockchain is secure.

ELAINE CHENG: Thanks. OK, so a little bit slightly different. And we know that it’s early days using this technology with blockchain, but it’s essentially, as you’ve described, open ledger. Can you talk a little bit about your thoughts related to privacy and any concerns with privacy or things that need to be considered in some of these blockchains around privacy?

CAMPBELL R. HARVEY: Yeah, sure. So, let me start with that voting application. So, it is a bit of a problem with a traditional blockchain application, because you cast your vote with your tokens. So, you get a token to vote. You can’t sell it. It’s kind of like the prescription — you can vote once, you can’t sell it, you can vote anywhere.

But if this is kind of a government organized blockchain, they get to see how you voted. So it’s probably not what you want. So again, this is a simple problem that has been solved, and it’s solved with a different technology. And it’s called a zero-knowledge proof. And my presentation, which I hope will be downloadable —

ELAINE CHENG: You can get in on the app. Everybody has it on the app.

CAMPBELL R. HARVEY: That — there’s an appendix on this. And essentially, what you can do is, you can prove that you’ve got the right to cast the vote without actually revealing your identity. It’s a very simple and elegant way to deal with that. So, that is not an issue.

And I talked about JP Morgan’s Quorum, where you don’t want other parties seeing transactions, your own business. So again, you can have the record of everything in a blockchain. But you have
a key to unlock the transactions that you are associated with. So, that ensures privacy. So, I think this is a great thing for privacy, just the cryptographic basis of this.

So, with cryptography, it’s very much in favor of us. So, we can easily encrypt something. But it’s really hard to decrypt if you don’t have a key. So, to actually go hack and to figure out the key is very, very difficult. In my medical example of the records, again, this actually helps privacy. Right now, everything is at risk. People can go in and gather this data that’s very sensitive and post it. So, I think that this actually has a nice balance in terms of the benefits of privacy and the costs.

ELAINE CHENG: Great. Thanks. OK, turning a little bit, we talked a little bit about the miners. And you talked a little bit, too, about the great benefits of getting rid of the middleman transaction costs. Can you talk a little bit about who will be the beneficiaries in establishing blockchains? Where will the profits go if there are any? And talk, maybe, just addressing some of the economics of what you’re saying.

CAMPBELL R. HARVEY: Yeah, so basically, what I recommend for every company, they need to have one person, at least, that’s familiar with blockchain, so a so-called blockchain czar. And that person is in charge of a couple of things. One is kind of an educational function, so a larger number of people in the company are educated on this technology. Number two, they need to figure out whether their business or part of their business is going to be disrupted with this technology. So, what are the weak points? What could we be disrupted on?

And then the last part is, what are the opportunities here? So, can we do something differently? Can we use a blockchain for our supply chain because the supply chain is causing a lot of problems? And you can you see this especially with food recalls, where somebody gets sick somewhere and they have to recall food over multiple states, right? With blockchain, you would isolate the particular stores that you need to recall. OK, so it’s a huge area in supply chain in actually implementing this.

So again, there will be losers. It is clear. But the beneficiaries are mainly us, the consumer. This means that we’ll be able to do things differently. This kind of machine-to-machine payments is another big deal. And you can imagine that people could make a lot of money — valuable people like everybody here. This is another source of income. And again, it’s directed to you rather than Facebook or Google. So, you earn the money for the information that you offer up.

So right now, it’s very inefficient. So, Google will kind of probabilistically identify certain characteristics of you. And that’s how they do the online auctions for the ads. So, the ad comes in. They’ve seen what you’ve searched before. And it is pushed to you. This is completely different than you actually offering your profile up, saying this is what I’m interested in. This is my demographic profile. You want to get to me, get to me directly? You’ve got to pay me.
OK, so these are pretty strong implications. It totally disrupts the usual way of thinking about marketing. Remember I said this course is not just a finance course? It is a marketing course. It is an operations course. It is an accounting course.

This idea is so general that it affects so many parts of business. But you need a blockchain czar at your firm. The consultants love this. So, all of the consultants have blockchain teams. And basically what they do, they go into the company and do the exercise that I just suggested. Said this is what you can do with blockchain. And, oh, pay us and we’ll implement it for you. OK, so they are basically playing the middleperson role. I think you can actually do this differently. Get somebody within your firm, designate them.

I remember one of my students took a summer job, so took the course in first year, took a summer job at a major law firm in New York. And it’s just like it’s a large law firm, many different interns. And he was doing just the boring stuff you usually do as an intern at a law firm. And then he’s tapped on the shoulder. Come with me.

And he’s taken into the senior partner’s office. He never even expected to meet the senior partner. And in the office, there’s somebody sitting, and he can’t see the face. But when the person turns around, it’s the CEO of one of the top five banks in the world. And the senior partner says we know you took this blockchain course. Explain it to us. Here’s a whiteboard.

[LAUGHTER]

Right, that’s the sort of power that’s possible here. So, that student got an offer — full time. And I know other students that have taken my course, they go in and quickly people realize they know something that everybody needs to know but they don’t know. And that gives you a huge amount of power to kind of do things.

ELAINE CHENG: OK, here’s another one. We’ve been extolling the virtues of the blockchain. Can you talk a little bit about maybe what you think the greatest deterrents are for adoption? Or what’s sort of blocking this happening? And maybe it’s a little bit of just understanding, but anything else you could say in terms of the blockages.

CAMPBELL R. HARVEY: Yeah, so this is a great issue. The first thing is that this technology is very young. So, that’s clear to everybody. And part of the reason I’m so excited about teaching this is that I like to teach things that will be relevant in the future. And there’s a lot of hype too. So, in my course — and I don’t mean to hype blockchain, though it might seem like it. That’s definitely not the case. You need to know — and I said right at the beginning of the presentation — you need to know the type of application. You need to be able to solve important problems. OK, so you need to be able to actually do that.
So, I think that the so-called killer app is where people are using the technology, but they don’t even know that they’re actually using it. So, it might be you’ve got your debit card, you’re swiping, you’re paying in US dollars to a merchant, but in the background, after that swipe, the dollars are translated into a cryptocurrency. The cryptocurrency is automatically transferred to the merchant and then translated back into dollars.

You don’t even know it’s happening. And that technology exists today to do in a very cheap way. The merchants would love for this to happen, because they are the ones that have to pay the 3%. Some of the other kind of areas… we thought initially that this would get a lot of traction with money transfer because money transfer is so expensive. It’s ridiculous. These firms like Western Union, 10% of what you’re transferring is their fee. So, we thought that would be kind of low-hanging fruit for people in developed countries transferring to emerging markets.

But a lot of the traction now is people in countries that are under stress, like Venezuela or even China, because it’s hard to transfer money out of China. So, there’s all this application that are possible today. But I think that it just has to be simple. There is a barrier to entry to really understanding this. I didn’t have to do the SHA-256. But I really wanted you to see that, so when you see it in the *Wall Street Journal*, you know what it is.

So you can have an even higher level understanding of this. But for this group, I think you need a deeper level understanding. And it helps you figure out what the applications will be that are possible, so everybody can be an innovator.

And the first time I taught the course, I had a mixture of business students, law students, engineers, and undergrads in computer science. And I was so nervous about putting the MBAs together with the computer scientists, the undergrads, right? I thought there’d be a lot of tension. But quickly there was no tension. The computer science students were a little nervous because they said Professor Harvey, does this mean we have to do all the coding? I said, no, you don’t need to do any coding.

So, there was a good synergy in that the computer science students had the techniques and many applications, but they didn’t know what was a good business application. So, they really leaned on the business students for their knowledge of a viable idea that’s actually profitable. And then the business students actually were using the computer science students, is this feasible to even do? So, you need this mixture. And I think that’s very important.

And indeed, when we have guest speakers in for my course, it is amazing that some of the leading people in the blockchain application space for the consulting firms don’t have a technical background. They’re not computer scientists, but they have a good sense. They can pick this up, and they’ve got a good sense of where this will apply in a profitable fashion.
ELAINE CHENG: Great. Kind of on that same train of thinking around application and where will these applications turn up, are you seeing any applications in the government around perhaps utilities, or services to citizens, and so forth? I know we talked a little bit about voting, but anything beyond that that you’re seeing?

CAMPBELL R. HARVEY: Yes, and there’s so many possible applications. For example, one of my projects was on government benefit programs. It is remarkable, the amount of waste, where people are being paid unemployment insurance when they have a job. OK, this technology makes it way more efficient for this to actually happen. So, many different levels of government are looking at this technology to improve disbursements and things like that.

Supply chain, I already mentioned. Again, it’s a nightmare of corruption. Maybe not as much in the US, but in other countries, it is a nightmare of corruption. Again, you have a supply chain blockchain. You can trace everything throughout. And it is secure. And if there is any funneling, then you see it right in that chain. So, governments are very interested in this.

ELAINE CHENG: Great. OK, we had a couple of questions. This change is a little bit... the track about, if we’re thinking about all this distributed computing, what kind of impact do we think that’s going to have on infrastructure, computing infrastructure? Do you see any concerns there, anything that’s different that needs to happen or change as a result of that?

CAMPBELL R. HARVEY: Yeah, so as I said, with the machine-to-machine transactions, this enables many different things. So, one of the cryptos that is recently launched — actually, I added to my glossary. I’ve got this glossary. I’ll put a plug in. It’s Harvey’s Financial Glossary in the iTunes store. I had to add a word. I’ve got 9,000 terms, but I had to add this word — I-C-O. So you know what IPO is, right? ICO is initial coin offering.

So, one of them that I followed quite closely is Gollum, as in The Lord of the Rings character. So, Gollum launched a coin. And basically this coin has got a particular use. And that is this computing application. So, you basically rent out, let’s say overnight, your CPU, and you’re paid in this cryptocurrency, and programs are run on that computer. There’s another coin that’s out there that is similar, Storj. And you can guess what it is. It is using some of your unused disk space.

So, you’ve got a terabyte drive — you can afford to essentially rent out 200 gigabytes. You get paid for it instantly. So again, this is happening. There are also very interesting things happening that I wish I had more time to talk about. The Chicago Mercantile Exchange, which I noticed they had a booth here, in the Royal Mint group are issuing a crypto based on gold. So, the idea is you take gold. It’s in the vault at the mint. And then you issue a coin that gives you the right to a fraction of that supply.

So, anybody could easily buy gold. You don’t need to buy an ETF, you don’t need to buy bullion, or coins. You can go buy 25 cents worth of gold instantly, with very low transaction fees. And
indeed, that crypto will not be as volatile as, let’s say Bitcoin or Ethereum. Bitcoin’s like six times the volatility of gold.

So, this coin will have a volatility that is gold. But you can think of using that for any transaction. So, you go in and pay for your groceries at Whole Foods in gold. It’s a great idea. But if you think kind of beyond this idea, think of doing this for anything. So you could take, let’s say a million shares of IBM. You put it in a secure vault. And then you issue a coin based upon IBM. OK, then in your wallet, you’ve got regular dollars. You’ve got your gold. You can pay for your groceries with a fraction of a share of IBM.

So, the vision that I never expected when I started out — this is the vision of a barter economy re-emerging. Wow! So, your phone’s got all the assets that are liquid, that have coin basically issued on them. And you’ve got your choice. So, there’s a lot of upside here that I haven’t explored in this presentation.

ELAINE CHENG: OK, I think we have time for one more quick question before we quit. So, I’ll end it with something kind of fun and maybe apropos for being here in the town of the US founding fathers. What do you think Alexander Hamilton would say about Bitcoin and the blockchain?

CAMPBELL R. HARVEY: Yeah, I think he would love it. And the person that I know would definitely love it is Milton Friedman, who actually advocated a rule in terms of the money supply. Keep it to a particular percentage growth every single year. In the Bitcoin algorithm, the amount of new Bitcoin created ends in 2140. Nothing new is created. So, it’s a deflationary currency in a way. It’s just a rule. It’s an algo. So, I think both of them would be OK with that because it really takes — when we’re talking about these public crypto, it takes the government out of the equation. The Fed, I doubt, would ever adopt something like Bitcoin or Ethereum. But when they do the Fedcoin, it does give them certain advantages.

So, the so-called helicopter drop of money for people is a really easy. It’s one line of code. Transfer $100 into every single citizen’s wallet. You’re done. OK, so this is possible. You can execute monetary policy very, very quickly.

The other thing that I remember, during this episode where Tim Cook refused to unlock an iPhone — do you remember that last year? And they threatened to put him in jail. And I told my students it would be the greatest thing for the only Duke CEO in the Fortune 500 to go to jail for this. But I also was shaking my head because to unlock an iPhone is trivial. My computer science students can do that. So, it’s kind of like questioning the FBI’s capabilities to actually do this? So, I thought there was some other game actually going on there.
But this is important. President Obama actually made a remark on this. And he said, well you know, there’s pluses and minuses here. And he didn’t think that it would be a good idea for, potentially, every citizen to have a Swiss bank account on their smartphone. OK, so I put that quote up in my class. And I said what do you think about that? And the student reaction is pretty swift. He doesn’t understand blockchain, because it’s not a Swiss bank account. You have Swiss bank on your smartphone. It’s your own bank. Everybody’s the same.

So, this is what this enables. And indeed, if you think, there are two billion people in the world right now that are unbanked. There’s a technology in Kenya right now that two-thirds of the GDP goes through, that basically uses your mobile phone to do transactions. And it is the mobile phone provider that is enabling the transfer. And they charge fairly large fees.

This technology allows everybody to be banked. And it’s easy to download these wallets, to do the transactions. It puts people that couldn’t usually access world markets into the game. It also allows people in developing countries — you’re in a village, you’ve got 190 IQ, but you don’t have the equality of opportunity, there’s no school. But they have a smartphone. Indeed, people buy a smartphone often before running water — a smartphone and a small solar panel. OK, so the ability to actually do some tasks, to write some code, to be compensated for it directly just opens up so many possibilities.

I talk about — I talked about earlier kind of driving by the cell phone tower and paying somebody that owns cell phone tower. Well, it might not be a person. It could be a group of people that actually own the cell phone tower. You drive by, and you’re paid instantly.

So, maybe you invest. Instead of buying 100 shares of IBM, you buy a piece of a self-driving Uber. And again, somebody gets in that car. They pay instantly. Money is transferred to your account instantly. So, the share economy is absolutely looking for this technology. There’s a lot of upside. But again, I do want to caution a bit, there is also hype. So, people don’t understand the technology. They create an application that looks really hot. But given what you know today, I think that you can actually go to some of those applications and say, well, this isn’t really a good idea, so that’s not really solving a problem.

So, the applications that are big winners are the ones where there’s a big problem being solved. So, we will see this, and over the next few years, many different applications — it’s going to get simpler. But for those of us that are actually thinking of investing or making strategic decisions at their firms in terms of what to do for the future, we need to know much more about this technology.

So, I encourage you to actually go to my website, take a look at beyond the first lecture. I go into much more detail, many more applications, and I think it’s a good investment in your time. Indeed, the CFA Institute is great at continuing education. So, you get your certification, but there’s always new stuff that’s coming out. There’s some depreciation in your CFA degree. And it’s
up to you to actually continue to educate yourself. And if you don’t, you might get left behind by somebody disrupting you.

ELAINE CHENG: All right, thank you so much. Let’s give Cam a round of applause — a great overview.