Blockchain as a tool for building an international registry of ownership for fine art

Authentication in Art Congress Wednesday 14.15, May 11, 2016

Prof Dr David Yermack

Albert Fingerhut Professor of Finance and Business Transformation – Stern University

Okay, first I would like to thank this great organization. Thank you very much for having me. Here we go. It has become clear in the last 15 minutes this is a very learned audience. I thought many of the questions were very provocative. I agree with, in fact, many of the premises of the speakers that, first of all, the art market is very amenable to economic analysis. People are extremely greedy and lawyers are all out to make a buck.

The second question, in particular, spoke about the need for trust. The big problem in this market is the lack of clarity and property rights, because people simply don't trust that the art is authentic and that the current person possessing the art has good title to it. What I'm here to talk about is a potential solution to this in the form of a new information technology. This is the so-called ‘blockchain’.

I would guess that many of you have been reading and hearing about the blockchain. I would also guess that very few of you have actually looked into the details and understood what it is and why it was created and how it could be used in the art market. This is what I'm here for today. The origins of this are rather surprising. The blockchain, as we'll talk about in a moment, was really created for this cryptocurrency Bitcoin, which has a very shadowy set of associations. It turns out that the technology behind Bitcoin, the way that you keep track of all the bitcoins, can be used to keep track of any financial asset.

The problem of trust is not at all unique to the art market. If you're buying a used car from somebody, you want to be sure they are the owner. If you're buying a house or a plot of land from somebody, you need to verify that they own the real estate. It's a very general problem in the law, how to show good title and demonstrate that you're the owner. This is a problem that, throughout history and markets of different kinds, has led to solutions that are often far from ideal.

What the blockchain seems to offer is a breakthrough in information technology that can solve this problem for all of these markets, if applied the right way. What exactly is it? The blockchain is basically a way of recording the ownership of an asset. Think of it as a little bit like a registry of deeds. It's an innovation. Some people have called this as significant as the arrival of double-entry bookkeeping which, about 500 years ago, really revolutionized the world of commerce and allowed people to keep track of assets in a way that was, basically, much more reliable than before, and set the stage for a long period of economic growth.

This is a totally different way than an accounting ledger of recording ownership. I think a good introduction to this, for those of you who are interested in following up, is a cover story in *The Economist* that ran last October. They called the blockchain a "trust machine". This gets at the issues raised by the speaker a few moments ago. If you can see the print here it says, "This is an innovation that carries significant stretching far beyond cryptocurrency. The blockchain lets people who have no particular confidence in each other," those would be your art dealer and art customer, "it allows them to collaborate without having to go through a neutral central authority. Simply put, it is a machine for creating trust."

I think this is exactly what is needed. If I could persuade you that this machine actually works, it might be very useful in the art market. What the blockchain really is, is just a sequence of transactions recorded in a certain way. This is an example taken from the world of bitcoins. Just so everybody knows what we're talking about, Bitcoin is a virtual currency. It's a currency that resides only in computer memory. There's no physical bitcoins. It's not issued by a central bank or a government but simply by a set of equations at a certain rate.

The problem with virtual money like this is, how can you be sure that people aren't copying it and counterfeiting it? How do you know that a person that shows up and says, "I have 11 bitcoins and I want to buy your car," how do you know that these are real bitcoins? The way you authenticate a Bitcoin is by tracing it back through all the people who have owned it from the point that it entered the system. It's not unlike buying a house where in the United States you would do a title search. I assume it's pretty much the same in other countries.

What you do with the bitcoins is record them as they're passed from person to person. You record them with a timestamp, which is critical. You would read this example from the bottom up.

What it simply shows is how many bitcoins are passed -- here's the quantity over here -- how many are passed from the buyer to the recipient. These are the digital addresses. What's in italics is the password that you have to enter, which is sometimes called the private key. Essentially, every time a Bitcoin changes hands, it is recorded in sequence with the timestamp. There is also a memo field here. We'll come back to this because in that memo field you can attach other information. What I'm going to suggest is that you could put an art object there to say, "I transferred a painting or a statue to somebody," then timestamp it and basically bake it into this blockchain forever.

Now, how does this get recorded? The blocks are collections of transactions. In the world of Bitcoin, every 10 minutes a new block is formed. They basically occur in sequence. This is block 10, block 11, block 12. What goes into each block is actually four things. One, and probably the obvious part, is the transaction data itself. Every 10 minutes, there's going to be something like 4,000 transactions somewhere in the world where people spend bitcoins. This basically shows from whom and to whom and how many bitcoins.

You also have the timestamp which tells you when the block was formed. This is very important because we want to know when the asset changed hands. You have something called the nonce. The nonce is a long random number. Think of trying to guess a 52-digit random number and how long that might take you. The reason that's there is because they want to screen out spammers, forgers, and hackers. If you want to create a new block in the blockchain, you actually compete with other people who are part of the network. Whoever guesses this nonce correctly gets to build the next block and actually gets a reward for doing that.

To guess this 52-digit random number, you need a supercomputer and it's going to take you about 10 minutes. This makes it very costly to try to come in and be a forger who would create false transactions and say, "All the bitcoins go to me." This is called proof of work in the information technology world. By introducing this proof of work, you raise the cost of forging very, very high.

Finally, you have the hash of the previous block. What a hash is, is basically a two-dimensional barcode. When you scan the product at the register, you scan the boarding pass to board the plane, you're familiar with these grids. A hash is a one-way type of cryptography where you can put stuff into a hash, but you cannot invert the hash necessarily to get back to what you had before. What you do is you hash one block into the next, then take all this and hash it into the next block. You end up with-- they've done a blockchain here where they're building this block and dropping it in after all these others have been done.

The problem in accounting is that people go back and erase stuff in the past and re-write history, as we say. This is exactly what we would worry about in the art market, that people would erase the title to art. In this example, what if you wanted to go back to this block and change it and say that you really own that painting?

You could do that, but then you would have to hash it into the next block and the next and the next. In other words, you would have to redo all the blocks that came after it, each of which involves guessing that 53-digit random number correctly. In other words, it's just infinitesimally likely that you could possibly do this before the next block is built successfully. This is a very clever marriage of some ideas in code breaking and information technology.

The other part of this, which is pretty essential, is that everybody gets a copy. In the world of Bitcoin, they have what is called a distributed ledger, which means that if you've got, in this case, four banks who are trading with each other, all of them get to see the roster of all the bitcoins. If somebody changes this block, everybody can see it being changed in real time. You have, literally, millions of sets of eyes on this, all of them going against the same copy.

By making it prohibitively costly to change the ledger by timestamping everything, and by creating, literally, countless numbers of monitors who will watch this happening, you make it impossible to rewrite history. This Bitcoin network has been up and running since 2009. There are issues with it and the behavior of people and what the bitcoins are used for, but it's been surprisingly resilient to hacking. It's a very robust system. What people have realized is that Bitcoin itself is really a curiosity, but this blockchain mechanism behind it is useful for zillions of potential things.

This recaps what I've said; that what you have here is a decentralized network, and you've taken the role of the gatekeeper totally out of the equation. Bitcoins can be exchanged peer-to-peer, and really any asset on a blockchain could be exchanged peer-to-peer, by relying on the code breaking mechanism to validate it and simply entering it into the block chain and waiting for it to be validated.

It's been shown pretty convincingly that once something is coded into the blockchain, it's there forever with the timestamp. This is exactly what you need to register property, and all the information that you might need in a court of law to prove ownership and approve the transfer of ownership at a certain time: a recording of the data at the time it occurred, with the identity of the buyer and the seller.

Another benefit is, is because this thing is decentralized, it runs on computers all over the world. You don't have to worry about the single point of failure with somebody hacking into the one computer of the stock exchange or the Central Bank. It's available around the clock, and ultimately the users control their own data. There has been a gold rush.

I use this in my business school class back at NYU where you've got a timeline, and it shows when different financial institutions begin to take up this technology and invest in it to adapt it to the markets for bonds, and commodities, and interest-rate swaps, and all kinds of financial products. In particular, in the second half of 2015, the real gold rush began. That was when the financial world really embraced this idea. You can't open the Financial Times or Wall Street Journal today without seeing about 10 articles about the latest blockchain.

In fact, this morning I read that the latest customer for this is NATO, which is using this for battlefield applications for secure communications. I think once the army starts using the blockchain, the demand for it will become almost unlimited. It gives it a certain imprimatur that even people are trusting this now in the national security area.

At this point, virtually every financial organization in the world is looking at how this can be adapted as a replacement for double-entry bookkeeping, to bring a totally different way of information, validation of ownership into the marketplace. It's a very exciting time.

Here's why we are interested in this: because almost any asset can be tracked on a blockchain that requires the recording of ownership. This is a schematic. I've just picked out some of the things that deal with intellectual property, in the arts, and so forth. Things like movie rights, copy rights, literature, and so forth. Obviously, transfers of works of fine art would fall into this category. I think in many ways, this is the ideal way to deal with the problem of trust. There's maybe more of a need for it in the art market than just about any other market that you could think of.

What are the issues in particular with art? How do you prove ownership, first of all? I think first and foremost, simply possession through history. That if you walk into a gallery with the painting, there's a presumption that it's yours. This is obviously rebuttable in court, but possession, in the art market more than many other markets, counts for validation of ownership.

Sometimes trusted third parties will validate ownership. For instance, insurance companies, by posting bonds or serving as escrows. There are certificates, but certificates can obviously be forged. The signature of the artist is a very crude way.

At least with some types of art, like with limited editions of Prince, people will number each one to prove authenticity. None of these methods is particularly good, though. It's very easy to see how you would get around almost any of these.

Now, what would you be able to do with the blockchain? If people registered all transactions on a blockchain, it really gets at these two big problems; that it would establish proof of ownership and transfer of ownership, and would also establish that the work wasn't forged. If someone forged something, obviously it would be painted later than the real painting. If they tried to enter it onto the block chain and there were two versions of the same thing, it would immediately raise questions.

What the blockchain gives you are these benefits that we spoke about a moment ago. That it's indelible and that you can't rewrite a record once it's there. It's there forever. The timestamp is critical, because you want to look at sequences of transactions and which occurred before others. It's almost free. With computer memory being what it is, you can run this thing at virtually no cost, and you don't need auditors, or experts or other people to be the gatekeeper.

You have numerous sets of eyes that will have access to the ledger that, if you would have a database, anybody could log into, which is the case with Bitcoin and many of these other currencies. It's immediately obvious when anybody is making an entry to change the ledger. A variation on this is the so-called smart contract. A smart contract is a contract written in computer code that executes itself if certain contingencies are met.

This doesn't always come up in the art world, but it does from time to time with things like licensing and royalties, the lending out of paintings, and so forth. I think there are some interesting applications down the road if the market goes in this direction, and I think frankly that everything is going to be on a blockchain in 10 or 20 years. There's probably room for these smart contracts to play a role in transferring ownership automatically, under certain contingencies. This would include people who pledged art as collateral for regular loans and so forth.

Now, what would actually be the way forward? What if people got interested in this and actually took this seriously and said, "We should start putting art in a big registry on the blockchain"? I think there are really three channels that you could work through, and each is really quite different.

One is that you could go back to that Bitcoin blockchain with the memo field that I spoke about before. Because you can transfer a nominal amount of Bitcoin, like .001 Bitcoin from yourself to another person, and attach to it 50 shares of General Electric, or your child's birth certificate, or the record of your passport. Anything that you want to encode as having been there at a certain point of time, and the title to an artwork is obviously one of the things that you could put onto a blockchain that's already there.

You could actually start doing this today. If you happen to want to buy a painting today, insist on coding the transaction into the blockchain. It can be done at very low cost and just go forward. There's a certain point of view, in fact, that the Bitcoin blockchain may eventually become the home not just to currencies, but to all assets. That the world may move toward a model of one big blockchain in the sky. This is a little bit intimidating, but in many ways it's the most appealing because it's already there, and we know that it works and you can free ride on it at a moment's notice.

A totally different model is to set up what is called a ‘permissioned’ or a ‘closed’ blockchain that would basically deal only in art. Rather than having this updated on a competitive basis by people around the world, you would nominate a trusted third party, such as maybe this organization, to be the master keeper of the registry. You would try to get galleries and museums, and private collectors all over the world to register their inventories on this, and especially register their transfers. It's a little bit like that registry of stolen art, except this is the opposite. This is the registry of good art that we know people have good title to.

What's critical to this is how much you really trust the third-party. What tends to happen with third-party gatekeepers is that they behave like monopolists, they take bribes, they sometimes get defeated in wars and people replace them with corrupt agents, etc. The whole point, in fact, with the blockchain was to decentralize this and make the third-party unnecessary. But one observes in the financial world today that this trusted third-party model is actually gaining some traction. I think you could have some reputable international body, maybe

UNESCO or somebody like that, start a blockchain for art and essentially run it for the benefit of world culture.

A third way forward, and there's a lot of activity in this area, is for entrepreneurial companies to simply go into this business and start running blockchains on their own. I quickly found three companies that are out there doing that, and then after I mailed in the slides I found that there's a fourth. There may be quite a few others, but what these farms are doing is exactly what I just described. They are inviting people to register their art for a fee, and then again for another fee, they will transfer; put in the record of transfer of title, and it will be timestamped and baked into a block chain in the way I described, so that it is always there.

I think if it were me, I might register my painting on all of these block chains and the Bitcoin one, just to give some redundancy to the whole exercise. But because this is information stored in the cloud, I don't think you have to worry about it disappearing. Once it's out there, it's there forever. I think that this, in many ways, is likely to bubble up from the bottom, because the technology seems very well suited to solving this problem. It's very low cost, and there are already people in a pretty high profile way competing to establish a presence in this market.

I think the question going forward is, which of these three is the most suitable? Or maybe even all three? Is there anywhere in the world a trusted third party who could do this for everybody? Or is this a problem best solved by competition among different data providers? Or do you want a free ride on blockchains that are already out there? I'm not sure really what the right answer is, but I expect that with fairly high probability you're going to see this migrate into the art world, because it's migrated into so many other financial markets within the last year or two in particularly interesting ways.