Podcast Transcript

BakerHostetler Blockchain University Bitcoin: Understanding the Phenomenon

Date: October 15, 2020

Guest: Rob Musiala, Joanna Wasick **Host:** Amy Kattman

Run Time: 26:35

For questions and comments contact:

Robert A. Musiala Jr.

Counsel
Chicago
T: 1.312.416.8192 | rmusiala@bakerlaw.com

Joanna F. Wasick

Partner
New York
T: 1.212.589.4635 | jwasick@bakerlaw.com

Kattman: Blockchain technology is widely anticipated to disrupt major industries and business operations over the next several years. But with all of the hype in the blockchain market, at times it can be difficult to separate fact from fiction and identify the real value in this new technology. To help bring things into focus, we've crafted a five-part series titled BakerHostetler Blockchain University to introduce blockchain from a technological, market and legal perspective. The second episode in the series focuses on the Bitcoin network, the world's first implementation of blockchain and the first cryptocurrency, Bitcoin. I'm Amy Kattman, and you're listening to BakerHosts.

Our guests today are Rob Musiala and Joanna Wasick. Rob is Counsel in BakerHostetler's Digital Assets and Data Management group, and the co-leader of our Blockchain Technologies and Digital Currency Team. Joanna is a Partner at BakerHostetler whose practice focuses on financial litigation, blockchain technology and cryptocurrencies.

Welcome to the show, Rob and Joanna.

Wasick: Thanks, Amy.

Musiala: Thanks, Amy. Nice to be here

Kattman: We know the Bitcoin network is the world's first implementation of blockchain technology. And Bitcoin is one of the world's most widely used cryptocurrencies. In many respects, the blockchain market started with Bitcoin, and so the origins and concepts underlying the Bitcoin network can provide insights into the issues that drive the larger blockchain market. There are just some really interesting stories surrounding the Bitcoin network, like the fact that we still don't know who actually created it. Joanna, where did the Bitcoin network come from? Who created it, and why?

Wasick: So, the idea of Bitcoin first came into the public domain in 2008, and that's when the Bitcoin white paper was written and published by the creator of the Bitcoin network, Satoshi Nakamoto. And Satoshi Nakamoto's white paper described a peer-to-peer version of digital money called Bitcoin that would allow payments to be sent directly from one party to another without going through a third party, like a bank or financial institution. And instead of that third party that would verify the payment, that role would be fulfilled essentially by a digital ledger that time-marks the existence and the movement of every bitcoin. And this is the description of a blockchain; a decentralized ledger that now is utilized in many different areas and industries. But here, it's a public, immutable, decentralized, digital ledger that's used to track and verify bitcoin. And it's free. There's no extra fee payment like you have to a third-party bank or a payment facilitator. And it's important to take this in the context of what's happening in the world when this white paper is being read for the first time.

Obviously, 2008 is a charged time for the financial world and the world in general. And these qualities of Bitcoin that are being described, especially the lack of a third party, is, it's crucial. While at many points in time a third party is something that's of value for financial transactions, at this point, when people's confidence in major institutions and governments is decreasing, having an alternative to that framework, that paradigm of needing the middleman and replacing it with a neutral piece of technology, that's groundbreaking and it's attractive.

So, the Bitcoin network itself comes into existence and functionality in January 2009. And that's when the first bitcoin is mined off the network by that same creator, Satoshi Nakamoto. And, Amy, you're right in your introduction. The thing is that nobody really knows who Satoshi is, period. Some people have speculated that it's one person, or it's a group of individuals known as Satoshi Nakamoto, that created Bitcoin. And there is even an article that was published in Newsweek that came out in 2014. And the reporter wrote that Satoshi was a 64-year-old guy living in Los Angeles, whose name actually was Dorian Satoshi Nakamoto. But this individual, Dorian, has emphatically denied that he's the Bitcoin creator. But there's another Australian computer scientist named Craig

Wright. Craig Wright, yep. And he claims he's the main guy behind a team under the pseudonym of Satoshi Nakamoto that created Bitcoin, but his claims are largely regarded as false by the media and the cryptocurrency community. So, again, we don't know who Satoshi is or was, and that really adds to the mystique about Bitcoin and the network in general. But, to be continued on that one. Maybe one day we'll find out.

Kattman: Well, we still may not know who created the network, but, Rob, perhaps you can tell us who controls the Bitcoin network.

Musiala: Well, the short answer is that no one controls it. If you have an internet connection, you can use the Bitcoin network to send and receive bitcoin and, really, no one can stop you, and that's the beauty of it. Although, it does create some legal complications, but we'll talk about those in a later podcast.

The more nuanced answer is that control of the Bitcoin network is spread out across the various people and entities that collectively support two things. The first is the source code, and the second is the mining hardware. And the fact that this control is spread out is what is meant when people say a distributed or a decentralized network. Really, any internet-based technology has two key components. First is the code that governs how the technology functions, and second is the hardware that processes the functions that are dictated by the code. And with traditional technologies, the code is written and controlled by a company and the hardware is a server that is also controlled by that company. And the Bitcoin network basically takes this model and turns it inside-out. In the Bitcoin network, the code is open-source, which means it's publicly available for anyone to see. Satoshi Nakamoto, whoever he or she or they were or is, wrote the code, but then Satoshi disappeared, and Satoshi handed the code to a group of five people who are now referred to as the Bitcoin Core developers. And the Core developers technically control the code because they're the only ones who can actually make updates to it. However, the entire world is watching this publicly-available code. And in fact, anyone can propose updates to the code, and that has happened. There's a formal process for proposing updates to the Bitcoin code. And at this point, there have actually been over 100 developers from all over the world that have contributed to the Bitcoin code. So, in this way, the code is effectively spread out across different people, or, you know, as people will say "decentralized."

With respect to the hardware, there's no single server for the Bitcoin network. Instead, there are hundreds, and actually probably thousands, of independent operators of hardware all over the world that collectively support the network. These are what are referred to as bitcoin miners. So, every 10 minutes, these miners race to solve complex algorithms that effectively verify and process transactions on the Bitcoin network. They do this because the miner that solves the algorithm first is rewarded with newly minted bitcoins. And interestingly, the more miners that compete to win this reward, the harder the algorithm becomes. So, now there's this huge industry devoted to bitcoin mining with companies all over the world that operate warehouses full of computer processors. And they're all trying to win these new bitcoins that are paid out every 10 minutes. And these

miners effectively take the place of a conventional server, so in this way, the hardware function of the Bitcoin network is spread out or distributed or decentralized among the community of bitcoin miners. One last thing on the topic of control that I want to mention is that there's this concept called the 51% Attack, which essentially means that if someone were to control 51% or more of the mining activity on the Bitcoin network, then they could theoretically manipulate transactions on the Bitcoin blockchain. And this is something to watch out for, but from a practical standpoint it's not too much of a concern because control of the mining industry is sufficiently spread out across, you know, various miners all over the world, and are, and is, you know, as they say, distributed or decentralized in this way.

Kattman: What gives Bitcoin its value, Rob?

Musiala: This is a great question, and I'll start by saying that I'll comment on what I call the inherent value of Bitcoin, and not the price of Bitcoin. If I was an expert on the price, I'd be doing this podcast from a vacation home in the Bahamas or somewhere. But the inherent value is, in my opinion, actually much more interesting. So, if you think about why the U.S. dollar has value, in my opinion, it's really two things. The first is that it's hard to counterfeit the U.S. dollar. We put a lot of money into making sure that the dollar is hard to counterfeit. If it were easy to counterfeit dollars, the value of the dollar would suffer greatly. And secondly, we trust the institutions and the systems that help us to store and transfer the dollar. So, if banks were constantly telling us that they lost all our money and we had to store all of our dollars under our mattress and pay for everything in person with cash, then all of a sudden, the dollar really starts to lose its value. And these same concepts apply with Bitcoin. So, so far it has proven impossible to counterfeit a bitcoin and, believe me, I'm sure there are lots of hackers who have tried. And so far, there has never been an instance where the Bitcoin network has been hacked or significantly disrupted, so the payment system of the Bitcoin network has proven to be very reliable. So, I often say that every day that goes by that a bitcoin isn't counterfeited, and every day that goes by that the Bitcoin network isn't hacked, the inherent value of Bitcoin grow stronger.

Now, I do want to point out that while the Bitcoin network has never been hacked, the individual wallets for storing bitcoin are very much susceptible to hacking and there have been a lot of instances of major hacks of individual Bitcoin wallets, especially from Exchanges. And there's even now an insurance, a whole insurance industry, dedicated to insuring against hacked bitcoins. However, while the Bitcoin wallets can be hacked, again the Bitcoin network itself that allows you to send and received bitcoin, that has never been hacked.

And then one other thing that I think gives Bitcoin its value is the fact that there is a readily accessible exchange market where you can buy and sell bitcoin in exchange for U.S. dollars or other national currencies. So, these days there are hundreds of cryptocurrency exchanges that are in the business of allowing people to sell their bitcoin for dollars or other currencies, or purchase bitcoin, you know, with U.S. dollars or other currencies. So, the fact that Bitcoin has become a relatively liquid market also, in my opinion, gives it inherent value.

Wasick: But, just to round out that idea, all of those qualities that Rob's talking about, that a bitcoin can't be counterfeited, that there's a means for exchanging it to other people for different types of value, that engenders confidence in people that this is a place where I want to store my wealth in. And so, having enough people storing their wealth or using it as a currency, that overall creates a valuable asset. And so, that's why you see people flocking to it more and more as a means of storing wealth.

Kattman: Joanna, Rob talked about who controls the Bitcoin network. Could you talk a little bit about who controls the supply of bitcoin?

Wasick: Sure. The supply, the amount of bitcoin that will be in circulation, that's controlled by the Bitcoin network protocol. And the numbers capped at 21 million. So that's the total number that will ever be produced, according to the code. And the way that that happens is that the protocol releases a block of code on the blockchain according to preset time increments. So, one block every 10 minutes. And that's where the bitcoins are coming from, for lack of a better term, and that's where they're mined from, the process that Rob was talking about earlier. And as time goes on, the amount of bitcoin that can be released or rewarded from these blocks is reduced every four years. And that's called a halving event. So there are less and less bitcoin available to miners as rewards as time goes on. So, when the Bitcoin was first launched, the reward was 50 bitcoin for solving the algorithm that Rob was talking about. And then in 2012 it was halved to 25 bitcoin, and 2016 it was halved again to 12.5, and then in this past May we had another halving event and the reward was halved to 6.25 bitcoin. So, the number is steadily decreasing, how many newly bitcoin are coming into circulation. And not only is that number going down, but the amount of processing, the amount of power it takes to mine and to figure out these algorithms is steadily getting more and more difficult. So, in the beginning, when mining was coming into an existence, you could basically do it off of, well, I couldn't do it off my laptop, but theoretically some people out there knew how to do this out of, you know, off their laptops, whereas now, you have a whole industry of companies that are consolidating computer computing power and different types of hardware so that they can rush and be the first to verify, the first to crack these algorithms, to get to this decreasing amount of newly created or newly mined bitcoin.

Musiala: Two points I want to add there, Amy, is that the mining market has really become kind of an arms race. As Joanna mentioned, the code base that governs the Bitcoin protocol is programmed such that the more people who are devoting processing power trying to win that reward of bitcoin that is paid out every 10 minutes, the more processing power that is devoted to that, the harder the algorithm gets to solve. And so that's why we now have this massive industry where you literally have these warehouses full of computer hardware that are devoted solely to winning that reward that's paid out every 10 minutes.

The other thing I want to note with reward to the supply of bitcoin is that because the amount of bitcoin is capped at 21 million, some people have concerns about supply-and-demand issues. But, in another sort of clever aspect of the code

base, the supply is, in many respects, governed by the users because each user is able to divide a bitcoin all the way down as small as eight decimal places. So, .00000001 bitcoins. And so, by giving the market, the users, the ability to slice and dice a bitcoin down into smaller and smaller pieces, that, in many respects, gives the market control over supply. And in fact, my understanding is that the code base can be updated if needed to allow bitcoin to be divided down even further beyond eight decimal places.

Kattman: And what is the current value of one bitcoin?

Wasick: I'll answer that. I think right now it's been about at $10,000 U.S. It's gone up as high, I think, about $20,000. It's reached $20,000 several years back. And initially, when they first came into an existence, they were in pennies, so the increase of value has really skyrocketed. And it's also created all of these different offshoots and different markets and different industries to support something of that type of value.

Kattman: Joanna, can you explain the other new markets that Bitcoin has created?

Wasick: Sure. And it's interesting, right, because initially when you go back to that 2008 white paper, part of the attraction to the Bitcoin design is the lack of third parties and the lack of this extra infrastructure. But as we see the value increasing and the amount of people who are purchasing bitcoin and using it, it's created, if not a need, *per se*, definitely a high demand for things to facilitate and safeguard bitcoin transactions and bitcoin custody and enable people to trade it more than just going on their computer and reaching out via peer-to-peer network to another individual. So, we spoke a little bit earlier about mining and how this is a new industry because of the computing power that's necessary now to get rewarded with these new bitcoins. But cryptocurrency exchanges, I think, are also a huge new market and these are businesses that allow customers to buy and sell cryptocurrencies, not just bitcoin, but it gives them a place to exchange bitcoin for other cryptocurrencies or other fiat currencies like a U.S. dollar. Basically, go to an exchange, you set up an account with that exchange and you can just purchase your cryptocurrency in that way, and you can trade it with other individuals who are also customers to that exchange. Once you have cryptocurrency, you need to store them, so there are things called wallets, and wallet providers offer services to store cryptocurrencies on behalf of their customers. And there are two primary types of wallets. There's hot wallets, and those are wallets that are connected to the internet and they have a private key that's managed by the wallet provider. These are the ones that are more popular on exchanges. So you'll open an account on an exchange, purchase your bitcoin and then keep it on the exchange as hot wallets, your hot wallet. But there are also cold wallets, and cold wallets store cryptocurrencies offline on external hardware, I think, devices. And although hot wallets are more liquid and user-friendly, cold wallets provide more security from hackers.

And then briefly, some other markets. There are cryptocurrency custody providers, and those are providers who supply storage services for cryptocurrencies in large quantities. And those customers are typically

exchanges themselves, high net-worth individuals, so, traditional financial institutions such as Fidelity and Northern Trust, who have begun initiatives to provide cryptocurrency custody services. There are also cryptocurrency payment processors who enable merchants to accept bitcoin on their sales, on their online sales. And then there are bitcoin ATMs which have been spreading quickly throughout the world, especially in the United States. And these are physical kiosks that look like traditional ATMs and the kiosk allows customers to insert cash and receive cryptocurrency. And users can also send their cryptocurrency to the kiosk's public key and then receive fiat cash from the machine, just similar to an ATM.

And the final market I'll touch on briefly, because they're becoming more popular, are cryptocurrency OTC desks, over-the-counter desks. And these are business that buy and sell cryptocurrencies for their own account, usually in large volumes. And the price volatility of bitcoin appears to have given rise to these types of firms, and they try to profit by buying and selling bitcoin at the right times. And OTC firms sometimes trade on cryptocurrency exchanges, but they mostly, I would say, deal in privately arranged peer-to-peer transactions, often with other OTC firms.

Kattman: Rob, as a final question, are bitcoin transactions anonymous?

Musiala: Great question. So, contrary to popular belief, bitcoin transactions are not anonymous. Instead, bitcoin transactions are what people call pseudo-anonymous, or what I'll call partially anonymous. For every bitcoin transaction that has ever taken place, since the very beginning of the Bitcoin network, there's a public record on the publicly available Bitcoin blockchain that shows the date and time of the transaction and the exact amount of the transaction. But here's the thing, the Bitcoin blockchain doesn't tell us the names of the parties to those transactions. And this is why I would call it partially anonymous. So instead, what the Bitcoin blockchain tells us is, it gives us what are called the public keys of the transaction parties. And a public key is basically a unique identifier, it's a unique string of letters and numbers, and so while we don't necessarily know who is behind a public key on the Bitcoin blockchain, with enough analysis of the blockchain data set, you can actually start to get a pretty good idea of the transactional activity that is associated with any given public key.

To dig a little bit deeper, these days there's this growing area, another growth area of the Bitcoin market, that are these blockchain analytics providers. And these providers have created tools that can be used to analyze the publicly available Bitcoin blockchain. These tools were originally developed to help law enforcement on investigations that involved bitcoin, but now they're starting to be used for more things. Things like anti-money laundering compliance for banks and cryptocurrency exchanges, and even for analyzing market trends and other economic trends. Part of the way that the tools work is they use what are called heuristic algorithms, which are basically advanced mathematical guesses. And they use these algorithms to show which public keys on the publicly available blockchain are likely to be owned or controlled by the same person or entity. They call these clusters of related bitcoin transactions or related Bitcoin public

keys. And the tools essentially group transactions on the Bitcoin blockchain together that are likely to be controlled by the same party. And then, when they do that, they can then start to identify relationships between these different clusters of transactions which would be relationships between different parties transacting on the Bitcoin blockchain. And so when you take these analytics tools and you combine them with other investigative techniques, things like searches of publicly available online information, social media, stuff like that, more and more we're finding that you can actually start to identify, with a fair degree of confidence, who's behind some of these semi-anonymous or partially anonymous public keys. By the way, the U.S. government has actually had some great success at using blockchain analytics to bust bad guys that are using bitcoin. So, blockchain analytics is really, a really interesting topic and it's probably going to become more and more interesting as time goes on and as use of the Bitcoin network continues to grow and become more mainstream.

Kattman: Thank you, Rob and Joanna. That was really interesting.

Wasick: Thanks, Amy.

Musiala: Thanks, Amy, always nice to be on the show.

Kattman:

If you have any questions for Rob or Joanna, their contact information is in the show notes. Be sure to check out our weekly Blockchain Monitor blog, where Rob is the editor and Joanna is a frequent contributor.

In our next episode of BakerHostetler Blockchain University, we will discuss the introduction to Ethereum, Hyperledger and other blockchains.