THE COMING SECOND WAVE OF DIGITAL & OTHER ELECTRONIC SIGNATURES IN COMMERCE

Panel: Ed Snow & Katy Blackwell

Moderated by Joan MacLeod Heminway

Joan M. Heminway: Thank you, Will, and thanks to all of you. A lot of you already know I am a business law professor here. This is actually my 19th year of teaching—a reflection that comes to me as I look out at some of my students from the early days in today's audience. We are all still in it together, folks. Welcome back to all of you and welcome to you if this is your first time at the College of Law. We are going to focus for this part of the session on digital signatures and on e-commerce and contracts. We have two really excellent presenters that I just met electronically and telephonically within the last few weeks. I got a chance to spend a little bit of time with Ed Snow in person last night. Their bios are in your packet, but I'll just say a brief word about each and it's not going to be what you read in their bios.

I happen to know that Ed likes looking at old literature on women scribes in Mesopatamia, Israel, and other places. We had a great conversation about that at dinner last night—he gave me heart that women lawyers have existed for an awful long time going back. Also, for those of you who are UT Law alums, he remembers being called on by Professor Aarons very, very early in his law career, and Professor Cornett, and some others on the UT Law faculty, too, with whom you may be familiar if you are UT Law alums.

Now, I can't continue with the UT Law theme with Katy, but I do understand, rumor has it, she has worked on an initial coin offering—something maybe during the breaks we will want to talk about, or it may even come up in the presentation as a way of making some analogies.

With those maybe more slightly personal introductions, I'm going to hand the podium over to Ed who will start us off, and then he'll hand it over to Katy, and then we'll all jump in on each other as needed, I suspect.

Ed Snow: Thank you for that. Can everyone hear me? Excellent. If you are not afraid to actually conduct business by electronic means at this point, then this will be a good session to listen and maybe give us some ideas and feedback about what you've seen and what you've experienced as we kind of work our way through electronic

signatures and in particular for a subset of electronic signatures that we call digital signatures, which is also a component of block chain. We are going to talk about the law surrounding electronics signatures. I'm going to talk about the pre-electronic signature law and how it's not really that significantly different, other than the medium. We are going to talk about the first wave of electronic signatures. For everyone who has been to Publix recently or used some other point of keypad to sign your name, maybe at Barnes and Noble somewhere, we've been doing that for a long time—or if you've purchased something from Amazon.

So far, there has not been a great move in mergers and acquisitions, on a really large scale, or corporate financings, to use electronic signatures, but all of that is changing. Some of my clients, who are national banks, now have swat teams examining whether or not they should start allowing their borrowers to start using Docu-Sign, for instance, or some other electronic signature company. They are trying to figure out what that means for them—whether or not they can attribute the signatures to the people who sign them and have remote closings. And really the truth is that I think that would be a more secure way of closing deals than we do now, because now if you've been involved in one of these deals, it's very rare to have a real closing in person in a conference room for 3 days where you get paper cuts, we eat soggy sandwiches, you have PTSD, Stockholm Syndrome sets in, you can't get out, everyone wants to get the deal done so you can leave. Now we close deals by email. It's rare that you see somebody's signed signature page that they send to you. You may not even know if they used Docu-Sign or not, or if they just took a stylus on their iPad and signed their name and took a picture of that and sent it to you and then we collect all of those. We try to have our electronic signatures and ink them too because then we require people to send us the ink signature pages afterward so that people can have inked hard copies in their file. The second wave, I think, that is going to come and is starting to come. We'll talk about that as well, and block chain of course plays an important part in that.

Pre-electronic signature law: Everyone has learned about the statute of frauds and that there are certain promises, in order to be enforceable, [that] have to be written, or a written memorandum has to be signed by the party to be charged. We all know about that. The key is intent, not necessarily the form the signature takes. I'm from Knoxville and I was raised on Gilligan's Island and Beverly Hillbillies and I remember, although someone has challenged me on this, Jed Clampett used to sign his documents with an X, which was his mark. Someone has challenged me on that so maybe Jed was someone who could write his signature. If you will recall from either that or some old movie,

someone signs and Xs their mark, and someone would witness that, and that was a valid signature. It was intended as a signature; you had a witness for that. In fact, I closed a deal in the 90s with Stevie Wonder, who was a party to the deal. He signed his documents with his thumb and fingerprint, and we set up signature blocks that said Stevie Wonder's thumb and fingerprint were intended as his signature and the witnesses signed as to that.

We also filed UCC financing statements with that and that was slightly difficult to do, because of the clerk of court, since back then you had to sign them. So we had to do some convincing, but those are valid signatures under the law. A signature stamp or a machine that's a signature machine, those are valid signatures as well. As we will see, that law really doesn't change—it's just a different medium. For instance, you can go back to the 1905 case in our materials from Nebraska. A court said "[a] signature is whatever mark, symbol, or device one may choose to employ as a representative of himself"[1] or herself. So that's a signature. There is a case as late as 1996 in the materials that talks about fax technology.[2] People used to worry about faxes and whether or not a fax could be a signature. In this case, it talks about a guarantee that someone sent. They didn't sign it individually, but at the top of the fax there was a header with that person's name. The question was: is that sufficient as a signature? The court found there was no intent.[3] That was printed and placed on everything that person sent, so that was not evidence of intent or a valid signature.[4]

With the emergence of electronic commerce, people started asking questions about whether or not a digital signature or an electronic signature was valid or enforceable. I did some research and found out that there is a claim. How many people have watched Halt and Catch Fire on AMC? It's a great show, it kinda goes through all of this. In the early 1970s, a couple of students at Stanford decided that they were going to transact business with some other students at MIT using their ARPAnet accounts. Apparently they sold some weed, and some people claim this was the first electronic transaction. The payment was not

---

[1] *Griffith v. Bonawitz*, 103 N.W. 327, 329 (Neb. 1905).

[2] *Parma Tile Mosaic & Marble Co. v. Estate of Short*, 87 N.Y.2d 524 (Ct. App. NY 1996).

[3] *Id.* at 528.

[4] *Id.*

done via electronic means—somehow they met in person or had some middle person, but some people claim that was the first one.[5]

I think it's more likely that this may be the first one. This was reported in the Smithsonian magazine when a man named Dan Kohn, who had a website called NetMarket, sold a Sting CD.[6] If you are a Sting fan, maybe some of you may be very proud, if not you are disappointed, but he sold it and also used electronic means to pay for [it]. That was thought to be the first one and that was in 1994. Then shortly after that, of course, Amazon comes on the scene, and we've all used Amazon probably.

With this first wave of e-commerce, the question was: would online contracts be enforceable? States started passing laws to make sure that it was enforceable. Some of the states chose very technologically specific descriptions of what would be enforceable. They were really concerned, because they were written by lawyers, that they might be too easily hacked so they were choosing digital signatures, many of them, as the means. But the industry decided that that's just too specific and maybe too hard of a threshold for people to conduct business. The National Conference of Commissioners on Uniform State Laws drafted the Uniform Electronic Transactions Act (UETA)[7], and that set a standard that was a little bit more liberal, more business friendly and the states started passing that but sometimes with nonuniformity. At this point, the feds got interested in this and decided to sign legislation called ESIGN, which was pre-emptive unless your state followed UETA with only some slight variations.[8] So ESIGN is pre-emptive unless you follow UETA. There are 3 states that have still have not followed UETA and if you have a transaction that's an electronic transaction and involve[s] New York, Illinois or Washington, you need to pay attention to those states. It's still up in the air, I think, what parts of those state statutes may be pre-empted. And I don't claim to be an expert on that by any means.

Here are some key points about ESIGN and UETA. I tend to just talk about UETA because they are virtually the same and if you are

---

[5] *See generally* JOHN MARKOFF, WHAT THE DORMOUSE SAID: HOW THE SIXTIES COUNTERCULTURE SHAPED THE PERSONAL COMPUTER INDUSTRY (2005).

[6] Marissa Fessenden, What Was the First Thing Sold on the Internet?, SMITHSONIAN MAGAZINE, Nov. 2015

[7] UNIFORM ELECTRONIC TRANSACTIONS ACT (1999).

[8] Electronic Signatures in Global and National Commerce Act, Pub. L. No. 106-229, § 102, 114 Stat 464 (2000).

in a state that has UETA then that's really all you have to look at. The key points are:

- A record or signature may not be denied legal effect solely because it's in electronic form.
- A contract may not be denied legal effect because an electronic record was used it its formation.
- If a law requires a record to be in writing, an electronic record satisfies the law.
- If a law requires a signature, an electronic signature satisfies the law.
- In a proceeding, evidence of a record or signature may not be excluded solely because it is in electronic form.

There is a lot of redundancy and overlap. You can tell that lawyers were really worried about making sure they covered the gaps. On these key points, again, UETA and ESIGN do not change contract law, but supplement contract law. As supplemented the law of contract formation, validity verification, authentication of signatures—those still have to be demonstrated if they are challenged. So that has not changed. In other words, pre-UETA and ESIGN signature law continues other than respect to the medium.

Here is a very important point that a lot of people forget, and I'll tell you an incident where someone forgot and regretted it. This applies to electronic records and electronic signatures relating to a transaction. That's what both of these acts refer to. A transaction is "an action or a set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs."[9] You might think that covers everything, but it has to be a transaction. There was a case in 2016 where a bankruptcy lawyer in California decided to sign some bankruptcy papers to be filed with the court using Docu-Sign. He did that and he was sanctioned. I don't know how grievous that was for him or how expensive that might have been, but he was sanctioned for that because it was not a transaction. The court has its own rules and regulations about what you do so you have to make sure if you are doing something and you want to use an electronic signature, that it's a transaction.

---

[9] UNIFORM ELECTRONIC TRANSACTIONS ACT § 2(16); see also Electronic Signatures in Global and National Commerce Act § 106(13).

The other thing you need to worry about is whetherh the parties have agreed to conduct business by electronic means. Usually this is obvious for the circumstances. If you go on Amazon, it's clear that they are using electronic means, and you've agreed to do that because of the circumstances. A lot of people I talked to, including some banks, and a lot of banks are looking at doing this, they are still worried that the electronic signature itself won't be enforceable. And my point to them is: that should not be your worry. Your worry should be that you just sent an email to a client in which your signature line might be interpreted as a signature, and you've agreed to extend a loan that you haven't approved yet. That's really where you should be concerned, not that it won't be enforceable but that something else you are doing might be a cautionary tale.

There are exclusions to ESIGN and UETA. Wills, condicils, testamentary trusts are excluded.[10] The UCC is excluded other than Articles 2 and 2A and some portions of Article 1.[11] Having said that, other sections of the UCC, other Articles have their own electronic signature provisions. Such as letters of credit, documents of title and security agreements of Article 9. Article 3 is the one that has not yet gotten on board. We're going to see here shortly that UETA and ESIGN have their own equivalent for a quasi-negotiable instrument that can be used via electronic means. There are other laws too that are excluded. I would categorize these under 2 types. Either something bad happened or there is bad news to deliver, and usually in a consumer context. So, if you have a clients who wants to send a notice about a recall of a product or cancellation of insurance and they want to do it by electronic means, you need to double check on that because that is excluded in UETA and ESIGN.

What do we mean by electronic? Well that's pretty easy but it's not just limited to electrical means, it's also optical, electromagnetic—it's open ended. What is an electronic signature? Again, this is the same type of statement you saw in that case from Nebraska in 1905.[12] It's a sound, symbol or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign.[13] It

---

[10] Electronic Signatures in Global and National Commerce Act §103(a)(1); UNIFORM ELECTRONIC TRANSACTIONS ACT § 3(b)(1).

[11] Electronic Signatures in Global and National Commerce Act §103(a)(3); UNIFORM ELECTRONIC TRANSACTIONS ACT § 3(b)(2).

[12] *See supra* at n. 2.

[13] Electronic Signatures in Global and National Commerce Act §106(5).

doesn't require a digital signature. We are going to talk about that, that is one of the highest and most secure ways of signing a document and making sure you can demonstrate attribution. What is a record? Well a record as used in UETA is both a tangible record and an electronic record.[14] An electronic record is created, generated, sent, communicated, received or stored by electronic means.[15] If you look at the comments to Section 2, it also includes a scanned document.[16] So scanned documents can be an electronic document. So you can take one that is paper and been inked and scan it. But there are risks in doing that and we'll talk about at least one or two of those risks. We talked about UETA creating an equivalent to a negotiable instrument and that's called a transferable record.[17] It's a subset of electronic records and it's something that would be a note if it were signed in writing under Article 3 or a document of title under Article 7 and the issuer, the maker, the promissor of the note, for instance in the context of a note, they would have to expressly agree that that instrument is a transferable record.[18] If you are ever going to do that, I would say that you need to make sure that's in the actual promissory note itself. But it doesn't limit it just to that; you can have a side agreement or some other agreement where the issuer agrees that it's a transferable record. The transferable record, if the party has control over the transferable record, and we won't really get into that today, that gives the holder some of the same protections that a holder of a negotiable instrument has not—every single one but most of them.

Here is one difference that I mentioned earlier. If you take an inked note and then scan it and the parties want to agree that that's a transferable record. UETA says you cannot do that. It has to be issued as an electronic record first. You can later paper out of the electronic record and create a paper note if the parties agree but you cannot have a promissory note that was signed in ink, scanned and then let that be a transferable record. You may still have an electronic record even if it's not a transferable record that is enforceable. I'll give you an example. There was a case in Tennessee, Synovus v. Paczko, in 2015.[19] The bank received an inked loan agreement that had a promise to pay, it was like a

---

[14] UNIFORM ELECTRONIC TRANSACTIONS ACT § 2(13).

[15] *Id.* at §2(7).

[16] *Id.* at §2(7) cmt. 6.

[17] *Id.* at §16(a).

[18] *Id.*

[19] Synovus v. Paczko, 86 U.C.C. Rep. Serv. 2d 746 (Tenn. Ct. App. 2015).

promissory note. That document turned up missing. Apparently it was destroyed by the bank. The borrower claimed that under UCC Article 3 destruction of the note can be evidence for discharge of the debt. And the bank said, "well hold on a second, look on page 3, there is a section of the note and it says 'the parties agree that the bank may take the original, manuscript signed inked note and destroy it and retain a PDF file of that note and the parties agree that will be enforceable between those 2 parties.'" And the court looked at that and said that was the intent of the party so it's not discharged debt. The court didn't get into whether or not it was a quasi-negotiable instrument but the court said it was enforceable. There was no defense to payment based solely on the fact that that inked note was scanned and then destroyed. Sometimes the question comes up whether transferable records or even electronic records can be collateral and how do you perfect on those. UETA takes care of this in the comments. It makes it clear that you perfect by filing because these are either accounts receivable or general intangibles. So filing of a financial statement is how you protect. Parties who get control may have the status of a quasi holder in due course, which has all sorts of great rights but that's not the same thing as a perfection of a security interest so you do it by filing. If you do both, that's obviously the better way to go if you have a lender who is ambitious and adventurous enough to make a loan based on those documents.

At this point I'm going to have a brief summary and then turn the time over to Katy. These electronic and digital contracts are governed by UETA or ESIGN but also always remember scope—have the parties agreed to conduct business by electronic means? I had a client ask me if they could take a whole stack of documents and just scan all of the loan documents going back to 1995 or something. The answer was no because the parties did not agree that they could do that, and those old documents did not have the provisions in them that said they would be enforceable as scans. So you've got to remember the scope of UETA. Also it has to be a transaction, otherwise it doesn't come within the purview of these acts. They also cover scanned contracts, electronically issued contracts, and also blockchain and smart contracts. With that, I'm going to turn the time over now to Katy and she will be able to discuss further digital contracts. Also we have a handout. Did the handout make the rounds?

Katy Blackwell: Okay guys, I'm going to start this off with a bang and just tell you I'm talking about technology but I'm horrible at using it so I don't know how the powerpoint is going to go. Electronic signatures, I'm going to talk increasingly in depth about digital signatures. So I want you to take from this slide, there is this umbrella of electronic

signatures, different types of them. It includes digital signatures but not all electronic signatures are digital. Digital is specific technology, it has international security standards, and advantages in legal evidence which we are going to get into. The statutory scheme doesn't require the use of digital signatures but it allows for them. There are plenty of e-signatures that are compliant and digital signatures are as well but digital signatures are more legally dispensable.

You have UETA's definition in here somewhere of security procedures. The point being to take from this, it's very broad, technologically neutral, it doesn't require specific security procedures to be used. So we need to know what security procedures are don't we? These are what you are going to look at for legal evidence. This is going to say, this is Katy's signature, she affixed it to the document and changes either were or weren't made to the document from creation to signing. There are various forms of these. The common ones are audit trails and it is what it sounds [like]. An audit trail is the record, the sequence of events that are recorded in the creation and the signing of a document. An important note that I think distinguishes e-signatures from digital signatures: digital signatures are going to give you a more comprehensive audit trail to look back on. It's going to record way more information and it's going to be embedded into the document itself. Just keep that in mind. You need, in the best case, an audit trail that is going to give you granular consistent and time stamped information of all of the events.

Authentication methods are things we've all used, this verifies identity and prevents fraud. Think of—you can do this with what you are—what you have, and what you know. So if anybody has ever unlocked their phone with a fingerprint or biomatrix, that's what you are. What you have would be something like, if a TFA was sent to your phone or using your passport or ID, and what you know would be answering these questions that you use when you set up an account, like what's your favorite pet, your mother's maiden name, and things like this. E-signatures, simple ones, may be authenticated but digital signatures must be. They are married, they are happy, you are not cute enough to break them up, important note.

Digital signatures, think of this as an electronic fingerprint. This is going to securely associate a signer and a document. This goes back to all of the information that is recorded and embedded into the document. Again, contracts with a simple e-signature, you are not going to get as much information, it's not going to be embedded into the document. You are often times going to have to go back to the provider or the website and say I need the legal evidence. What happens if they go out of business, well that's a little more complicated.

I want you to pull out the handout that we discussed, it looks like this but it doesn't have coffee on it, probably. It's the evolution of a signature and you see 3 columns. On the left you have a traditional signature, that's your ink and paper. The middle is what I call a typical e-signature. The right side is PKI digital signatures. The gray tile that you see is what speaks to your legal evidence. This is what you are going to go back to. In the middle, you see a typical e-signature and we see one gray tile. So you have a PDF, you have signature images, they are placed on top of the PDF, then you have a tamper evidence seal and that's really the only information you are going to get and you are going to have to go beg the provider for it. It's not a lot. So when you get to PKI digital signatures, what's important to know about this, not only is there way more information, but it's for every event or every signature, whether it be 2 signatures or 10. You are going to get the signature image, the name, transaction ID's, browser information, certificates and tamper seals for every one of those signatures. And I'm going to keep saying this, it's embedded in the document.

Joan M. Heminway: So Katy, can I just ask a question about that? I think, for a lot of us, we are very familiar with what Ed described before: the in-person closing. Some of us are of that age here…. But even tthose of us in that advanced age group also are familiar with the electronic closing, in which there is verification of an actual electronic signature afterward. At either of these kinds of closing, you might have, for example, a secretary's certificate, with an incumbency certificate certifying that that a specific person is authorized to sign specific documents. I think what you are saying here—and you tell me if I'm wrong about this—is that in with digital signatures, those kinds of evidence of the verification of a signature and the signatory status are unnecessary.

Katy Blackwell: Yes. And I'm going to get into how this works and I'm going to try to explain this on a high level because it's complicated.

Ed Snow: I would also add too that I don't think banks or other transaction parties will dispense with the officer certificates because you still want to have certification that the board or the members of an LLC met. You may still want an incumbency certificate, but it's not going to be a manual signature, it might be something completely different in the future. It might be a certification from a service provider or something else like that. We are still kind of trying to make this up as we go because people haven't really done it extensively in commercial lending or M&A transactions. But those are also a part of a security procedure,

that is to have these incumbency certificates or an officer certificate and those are also admissible.

Katy Blackwell: Great. Thanks. So I want to explain to you, how digital signatures work. It's called PKI technology. It stands for Public Key Infrastructure and it involves two keys. Keys are very long strings of letters and numbers. You don't memorize them, you don't write them down and keep them in your back pocket. They operate invisibly and magically to do things for us pretty much as far as we are concerned. You have a public key and a private key. You can't do something with just one of them, they have to work in harmony. They are mathematically related. I'm going to give you an example in a minute of how this all ties together in a blockchain but for time sake and for now I'm going to tell you this is military grade cryptography, i.e., it's a big deal. This is what gives you the multiple layers of proof and this is why you have them embedded into the document and you don't have to go back to anybody and ask for it later.

Some industries haven't wildly adopted the use of digital signatures yet. There are different reasons for that and I think I could speak more comprehensibly on it. I think some industries like banking just really like ink documents or they may require them for collateral. They might not have the capacity to store a high-volume, securely, of electronic records of the long term, which a blockchain could help with, we'll talk about it in a minute. And they may not think that the signature is going to be upheld as being legally valid, which is what we are seeing, they are. I can tell you, we work with clients in wealth management, really high-value contracts, real estate, and maybe most compelling, clinical trials, a company that manages hundreds of clinical trials and they use PKI digital signatures, they trust them. So I think it could work for a commercial loan.

I want to go over briefly some things about blockchain. We are not going to get too in depth about it, but I'll give you a very generic definition. It is a distributive ledger where transactions are recorded and linked, so you get the entire history of an asset. What does this have to do with digital signatures? The blockchain requires them in order to operate. Put it in a different way, digital signatures are required for every ledger entry onto the blockchain. This is where I want to give you an example. How many of you have ever bought cryptocurrency or transferred it, bitcoin or anything, in any way? For those of you who haven't, I think this will still make sense. This is when PKI comes to play, blockchain and all of these security procedures.

Let's say, I'm going to transfer a bitcoin to Ed, which is not going to happen, but you need to buy into this generous character that I'm giving myself. So I'm going to transfer a bitcoin to him. I first need a wallet, it's like your bank account. So I create a wallet and when I do three things happen. I get a wallet address, which is this long string of numbers and letters. Then I get a public and a private key, there is your PKI coming to save the day. So these are all mathematically related again. I am not going to get into it because I couldn't explain the math but I can tell you that the public key comes from the wallet address. We are going to put it aside for now, we don't need it yet.

So I log into my account, user name and password, to send this bitcoin. And when I do, my private key is encrypted down in this wallet somewhere invisibly. I log in and the private key decrypts. I want to say that it wakes up and is ready to go to do something. Then I say "Wallet, send a bitcoin to Ed, here is his wallet address, go." And that private key digitally signs the instructions that I just gave, but the transaction can't complete yet because you need the public key. The instructions are sent to the blockchain, bitcoin, my public key is out there somewhere and it matches everything up—all of these make sense. And I think you know what I'm talking about and I may be a little bit wrong on this. It matches everything up and when it does, validate, validate, validate and he's got a bitcoin in his wallet.

Let's say I sent a bitcoin to some nefarious shady character that committed some unspecified crime and you come to me and you say why are you funding a criminal enterprise? And I'm gonna say, I'm not, you're crazy. And maybe you are going to be clever and say but your private key that is encrypted in your wallet that you have access to, signed the instructions and then it was validated on the blockchain, so yes it was you. And what am I going to say, does anybody have a guess? "I was hacked and it wasn't me and you're crazy." So then what, security procedures. Think about how this works with digital signatures. What I didn't tell you is when I logged into my wallet, user name and password, it said hold on a minute, we are not letting you in, there is a two-factor authentication code sent to your phone, give us a code. I say okay here is the code and I say send the bitcoin to the baddie. It says well wait, we sent a link to your email, we need you to click on that link because what does that do? That says, I am Katy and I'm telling you to send the bitcoin to the baddie. The transaction will complete as I described. But that's how the securities procedures tie in to the PKI digital signatures. It's important to know that you need at least a couple of authentication methods when you are doing things like this. That's how it all works together. I hope it makes sense.

Smart contracts also operate on the blockchain, these are protocols that are used, they are smart and they are contracts, so that's not a clever name. They are smart because you can write into the code predetermined conditions to tell it what to do and it will do it by itself. So think of, very simplistically, write into a code "if X then Y," and that's what it will do. There are a lot of applications for this, you have a bank loan example. Let me tell you what I do on a daily basis. We're taking digitally signed contracts, various subject matters, and we are linking them to smart contracts on the blockchain. So then what happens? Key terms and conditions of these existing contracts will automatically be executed without more manual intervention. Saves you time, saves you money, all of that good stuff. You could put a car loan into a smart contract such that when you default there is a lien that just magically comes out of nowhere. If I'm going to buy goods from you and I say, "I want this by October 3rd, if I don't get it then I want a refund." If no package by October 3rd, write it in the code if there is no package by this date, this amount of money comes back to my account; October 3rd comes, no package because he just did not mail me what he promised and I have a refund in my account. Smart contracts depend on digital signatures.

More benefits of the blockchain. This speaks to the security and the mutability. This speaks to the identity verification. Going back to the bank example, they would be able to better comply with anti-money laundering and your customer requirements. Put that on individual side and we guard against identity theft. To tie it up, the statutory scheme that exists seems to contemplate blockchain and smart contracts such that they would have legal effect and there is some debate on this. But you get definitions of terms like electronic agents and automated transactions. I think an automated transaction is a smart contract, but just to be sure, some states have an enacted their own legislation to be more specific and to make sure that these have legal effect. Tennessee is one of them. Joan has more familiarity with that so if you want to chime in and share some of your specific knowledge.

Joan M. Heminway: I'm happy to do that. The Tennessee General Assembly, as you may all recall, if you have been reading the newspaper, enacted one of these specialized statutes that recognizes as digital signatures "[a] cryptographic signature that is generated and stored through distributed ledger technology."[20] I am a member of the Tennessee Bar Association's Business Law Section Executive Council.

[20] TENN. CODE ANN. § 47-10-202 (2019).

We were given the draft of that statute. It was originally modeled after an Arizona statute, which is one of the other states that adopted a statute of this kind back in 2017.[21] We were given 24 hours to comment on it. For those of you who are familiar with the legislative process, this is not odd but it is not normal either. Typically, when a sponsor of a bill puts a bill forward, you have some time to digest it and discuss it. In fact, in this case, the bill was filed in January, but it was not until February that we were called and asked to comment on it—for a hearing in two days. A consensus bill emerged from that brief review period. With both the bar looking at it (very quickly) and also the National Technology Council, the original bill was substantially changed.

I will to let Ed talk about his critique of these statues in a minute. I am very familiar with the critiques of these statutes, not Ed's particularly. However, there is a faculty member at St. Mary's Law—a woman by the name of Angel Walch (who was formerly paralegal in the office in which I practiced)—who is a blockchain expert affiliated with various blockchain organizations who is very critical of our statute and came out in the press saying, effectively, if not actually, that "it looks like they threw the kitchen sink in" on the definition of distributed ledger technology (because the Tennessee statute is not just meant for blockchain).[22] The Tennessee statute covers any application of distributed ledger technology that might generate and store cryptographic signatures. So, that term in our statute was given a very broad definition. It was intended to be very broad to bless any kind of cryptographic signature on any kind of transaction that takes place. That was the intent of the original drafters and that was what we were asked to help effectuate through our review as representatives of the bar. None of us felt very comfortable with it, I can assure you, given the short amount of time that we had to review, deliberate, and discuss. We had to try and scramble to find people to help us to comment on the bill. It was not a perfect process.

I want to just give you a slice of life in relating this story—specifically, the life of those engaged in legislative drafting, proposing, and revision. We do not have formal legislative history in Tennessee (except for hearing recordings), which actually can be helpful. However, in commenting on the bill, one of the folks from the Greater Nashville

---

[21] *See* ARIZ. REV. STAT. ANN. § 44-7061 (2019).

[22] *See* Adrianne Jeffries, *Blockchain Laws Tend to be Hasty, Unnecessary, and Extremely Thirsty* (March 29, 2018), https://www.theverge.com/2018/3/29/17176596/blockchain-bitcoin-cryptocurrency-state-law-legislation (quoting Professor Angela Walch).

Technology Council wrote to basically say it was the philosophy of that organization, in commenting on this statute, that they join the bill sponsors and the house and the senate in wanting to hang an "open for blockchain business" sign at Tennessee's door—a view widely held by others.[23] Tennessee wanted to be on the front end of any statutory adoptions. What this means sometimes is, in your haste to get something done quickly, you do not get it quite right. So the critique that Angela Walch, my colleague from St. Mary's Law, made was, in essence, that the statutpry definition of distributed ledger technology looks overly broad which could be great for business but may really hang things up in the courts because it is not very clear in application. The fear of the Tennessee Bar Association administration, as well as the Greater Nashville Technology Council, was that if you enact a statute like this, you would actually potentially narrow the preexisting electronic signature statues which a lot of people thought were already applicable to blockchain transactions and transactions that may be conducted in other distributed ledger technology formats that might arise or have already actually been invented.

In sum, there is a difference in this kind of lawmaking effort between the Tennessee legislature wanting to be open for business and those of us who are typically more cautious about legislative enactments. One of the reasons why bank and M&A transactions are not yet done in a blockchain is that we are cautious lawyers, we're the old school lawyers in a lot of ways. In my experience, legal counsel who represent banks or firms in M&A tend to be a little bit more conservative in making legal judgments than attorneys in some other areas of practice. That may just be my observation, but I do think that's part of what is behind some legislative tensions.

I did not want to have to comment on the cryptographic signature statute in 24 hours with my colleagues and, in the process, try to anticipate and navigate around what a court might do with a law of this kind. But the train had left the station; we understood the legislation was to pass, regardless. This happens from time to time with legislative actions: a bill is going to pass, and you have 24 hours to make it a little bit better (or to better effectuate at least the policy underpinnings of the

---

[23] *See*, *e.g.*, Jeannie Naujeck, *Blockchain Tech 'Is the Shiny New Penny'* (May 18, 2018), https://www.tnledger.com/editorial/Article.aspx?id=106706; Waller, *Tennessee Takes Leadership Role in Support of Blockchain to Attract More Businesses* (Nov. 6, 2018), https://www.bizjournals.com/nashville/news/2018/11/06/tennessee-takes-leadership-role-in-support-of.html.

statute). Alternatively, you miss your opportunity and it could be disastrous because the bill's provisions do not match, for example, Tennessee law (typically because the proponents are using a model from another state). That's the conundrum that we were caught in with the digitial signature bill. I wanted you all to know about the background. So, if you find the statute frustrating, go ahead and try to blame me; but just understand that we all had, as a group, 24 hours and it was an exercise in "sausage making"; no individual in the group got everything he or she wanted, and there is a lot of stuff in there from a lot of different players that was added very quickly. Ed, maybe you'll now want to say a word about your critique of these statutes.

Ed Snow: Sure. And we both agree as to the risks with enacting this type of statute. There is an industry association called Electronic Signatures and Records Association, which has the very clever acronym ESRA. ESRA was a scribe in the Hebrew Bible so that's kind of cool I think. They came out against adding this type of statute because they took the position and made this position known that they think the language in UETA governing electronic agents is sufficient. Again, the risk is you may make it too narrow. If you are going to do something, it should probably be an amendment to UETA that says "electronic agents includes without limitation the use of a distributed ledger of technology."

I think the other thing to remember too is that right now, at least based upon what I've read, and I haven't seen this, is that the people who are using a smart contract, that really doesn't exist on its own outside and independent of a written agreement, but is a part of a contract. And the remedies in the smart contract--or a code remedy—is also set forth in English in the contract that someone has agreed to in writing, and which they've read. They may have signed it by electronic or digital signature, but the code is the smart contract that operates and effects the remedy that the written contract says the parties are entitled to. That raises all sorts of questions and I think this afternoon, the next panel may discuss that, but in my mind as a banking lawyer, if the smart contract remedy happens one day after the party to be charged has filed bankruptcy then that violates the automatic stay. So there are all sorts of statutory schemes that need to be reanalyzed and looked at so that the technology that's moving so quickly won't have problems by virtue of the law, the law has not kept up with this area.

I would add one other thing, too. I'm a big believer in the digital signature technology and Signix is a great company and I'll make a small advertisement for them. You shouldn't be completely terrified of using some other signature company that doesn't have digital signatures. If

you do use them make sure that they have at least dual-factor authentication. What would that be? Katy's already talked about that but it could be as easy as the person who is signing also gets a number texted to them and then they send it back to the service provider's platform so that the service provider has that in the audit trail, reflecting the dual-factor authorization. So when you go to court and that person claims they didn't sign it, then you can bring that service provider as a witness, if they are still in business, and if their documents they saved on their system are still available, they can come in and testify. And then you also as the attorney or the business person can also testify. I've been working with this person for 6 months to close the deal. I have emails from them that morning that they were going to sign the document and send it to me and then I got this and this was their cell number, that was in an information certificate that I got at closing, that is their number and it was sent to them. Then they signed it by means of clicking on that as the final step. Those are the security procedures that we were talking about.

Again, UETA has the advantage of being very open-ended and liberal in its construction and it includes all these things. The digital signature, which is the key to the second wave of blockchain transactions, you have to have that and I think that that will become something more available to people and eventually people will be using their digital signature, not just for one transaction but for multiple transactions, just like they use their own ink signature.

Joan M. Heminway: Before we get to questions, I will add that one of the things that drove the Tennessee bill also was the people were already using blockchain in, for example, the healthcare industry and a number of other industries in the state that carried a lot of weight. Some of these folks probably had put some public interest pressure \ on the sponsors of the bill to get something adopted because they were concerned that the transactions that they were engaging in ordinary commerce used cryptographic signatures and might not be given effect. As a result, they wanted to make sure that Tennessee law was not behind in that aspect. I got the sense of that from reading additional articles to prepare for this panel. One of the reasons why we had to then broaden our language in Tennessee bill that I earlier failed to mention was that the Arizona legislation related only to blockchain and the reason for that was that it was a statute focused on cryptocurrencies. We were not trying to do this for merely for cryptocurrency reasons, but rather for more general commercial reasons related to industries that were important to the state. Hopefully that helps a little bit to fill out the picture.

Okay. Now, we would love to take questions from the audience for the remaining 10-15 minutes of our program, if you have them.

Audience: *Do you foresee potentially any changes to UETA, or any provisions to it? As we see, especially with the expansion of where it applies and where it doesn't.*

Ed Snow: I'll say this—this is kind of answering your question—I do see that on the one hand. On the other hand, crypto currencies nowadays are assets and mostly individuals own them, but my sense is companies may start owning them—your company could invest in some else's ICO for instance. That raises all sorts of questions, including is that crytpo currency a part of the banks collateral?

I'm a bank lawyer, I'm going to see can we foreclose on that. Well, foreclosing on it is one thing, but it's clear you can get a security interest in it because it is, no doubt, just like these transferable records and electronic records, a general intangible. If you file a lien against all assets of a company, you've got that. Now, if you are going to foreclose on it, you have to be able to find it and be able to transfer it. And how are you going to do that? Well, some banks may say, "I'll tell you what, you've got some ether or bitcoin, well I want a security interest in that and you are going to give me your private key and public key information," basically the password to your account and if the bank loses that, this is not like Facebook where you can contact someone and retrieve your password. Everyone has read about these people who bought bitcoin ten years ago and they lost their password or sold their computer and lost all that money.

There is pending legislation where Article 8 of the UCC will be amended possibly to allow you to have a control agreement--just like you do with a deposit account or a securities account, and you can be perfected on the money in the deposit account or the securities held on the securities account—and under the proposed legislation, the crypto control agreement will be with a crypto exchange. So it will be secured party, debtor, and the exchange. You will sign a three party agreement, a control agreement. You are not perfected on the individual crypto currency in the account, you are perfected on the account. That way the bank or the secured party doesn't have to dirty their hands with holding on to the password and they just send notice. That can all be done on a blockchain as well.

That's what I see happening. I don't get the sense that people are going to completely overhaul UETA. If you wanted to make it clear that smart contracts are covered, I would do the including without limitation add-on to what's existing. Anything else?

Katy Blackwell: Well, I have a question for you. If the banks get an interest in the crypto currency, is that the value of it on the day?

Ed Snow: Well, that's another question, whether or not, and maybe Tom Potter is going to talk about this this afternoon, about people who are crazy enough to lend on crypto currencies. Most banks today that I've talked to, it's usually the workout group of the bank that was interested. It's like okay yeah we are foreclosing now and there is a deficiency of a loan balance, is there anything left? Well, they might have crypto currency. How do I get to that? Good luck. You might have a power of attorney in your loan documents that might enable you to get access to it somehow. Basically, most banks right now are not including the value of the crypto currency if they are lending against or even thinking about it, part of maybe a borrowing base or they are not giving value to that as a part of their lending. But there are some platforms that are active in Europe that are trying to do this in the United States where they are actually lending against crypto. The problem is that you will be regulated. To do this, you either have to be a bank or you have to be regulated by the CFTC. Nobody wants to be regulated by the CFTC so they try and figure out another way to do that, possibly a structure that is not really a margin loan, but possibly a short term repo. And Tom may talk about that later today, so I'm going to shut up.

Joan M. Heminway: Does anybody in the audience do family practice of any kind? Maybe divorces, trust and estates work? Hear what Ed is saying about assets, valuing assets, keeping track of assets, and what all of that has to do with cryptocurrency. Because blockchain tokens and coins represent interests in assets, lawyers in those fields are going to want to know about this technology, as well as attorneys who are doing banking, M&A, maybe what we call traditional corporate transactions. Valuation, finding out the value of a cryptocurrency—what's held in their wallet—is important to practice in all of these areas. How does a lawyer know what's held in the wallet of a client or a spouse in a marital relationship? It is not like couples are going to necessarily give each other their public and private keys and have access to each other's wallets all the time.

Ed Snow: Or even know those wallets exist.

Joan M. Heminway: Exactly. Next question from the audience?

Audience: *Hi. My question is for either of you regarding the way that smart contracts work to the extent that as I understand it because I don't know anything about this. Programming is going to be used to ensure that certain activity won't happen or it will happen automatically and having lived with a person who does*

software work and has done so for over 20 years. I know that people create problems inadvertently and we call them bugs. And when that happens in the context of a smart contract, if there is something that requires debugging how do you avoid an amendment to a contract without necessarily permission to the extent that damages occur because there was something that happened inadvertently that caused damage to one party or the other. How is that handled in a smart contract?

Ed Snow: I'll say one thing because I always feel the need to say one thing and then defer to the next session. From what I've read, there is a great business opportunity for audit companies or bug bounty hunters to go in and fix bugs because apparently these smart contracts are being written so quickly that they have three times as many bugs as normal code. And you are exactly right, that's a big problem. You have to test them, you have to make sure they work. I usually refer to a vending machine as an example in real life of how a smart contract could work. You walk up to the vending machine, you put in your dollar, you put in the right code for the potato chips, the potato chips come out. But sometimes the potato chips don't come down and they are hung up there and you are shaking the machine at the risk of your own life with the machine falling on you and that's exactly what can happen and people could spend all this money on creating it but if they don't test it to make sure it's debugged then that's a problem. I hadn't thought about the damages, that's a great point.

Joan M. Heminway: And you may have heard that the blockchain is secure. We don't have an intermediary who can make mistakes, but you are pointing out the area where those mistakes can be made—through the coding.

Audience: *Question about the smart contract. I was talking with a friend before this segment and I understand the cost per transaction on smart contracts is a little high. I was gonna ask, as you add all the notes to the blockchain to some extent you have a reverse economic scale because it gets more expensive as you add all these notes to update the ledgers across the blockchain. How are your clients coming to you and justifying, do you expect the transaction cost to drop or do you have any comments?*

Katy Blackwell: Yeah, we do but won't don't have this live and working yet. It's still in this test phase. Still at these hackathon phase where we are trying to work out all the bugs and see if it's really going to work out in the long term. A lot of our clients are some of the top wealth management companies, real estate companies and things like that. We are using them as a test run to work out some of the things that you are talking about.

Ed Snow: In the finance realm I think that you will see blockchain as a service develop fairly quickly, for finance, for trade finance with letters of credit and for trading syndicated loans on a blockchain, and those I think will be offered like you can buy any software off the shelf. I think the scale will be there very quickly. Anything that's bespoke, I think there is a lot of cost in that. I also think you are speaking about the energy cost and a proof of work consensus mechanism. A lot of these blockchains that I've read about will be private ones among banks for instance that are permissioned and they use proof of stake or some other type of consensus mechanism, they won't have some other type of cost, at least that's the thought.

Audience: *You said you had a prototype, are you using a public and private application?*

Katy Blackwell: All of the above. Public, private and then a hybrid of both.

Audience: *You were talking about authentication and I was curious to find that you can use electronic sound as a signature. Do you see any use of you know now we can send a text with our voice, we would be using sound to agree to the contract as an electronic signature with your voice?*

Ed Snow: I want to see that before I retire.

Katy Blackwell: I think that it could be done, I don't know how you would verify that though.

Ed Snow: We also had Prince who used a symbol as his name. I heard through the grapevine that he closed deals with that symbol created in WordPerfect for documents.

Audience: *There is enough science into voice technology where it's actually as unique as a fingerprint. The problem is the technology is not there yet. So to be able to implement it would be very hard at this point.*

Joan M. Heminway: I have one if nobody else has one. Katy, you said smart contracts are both smart and contracts. There was someone who said exactly the opposite at another conference that I was at, at the Tennessee Bar Association, and made an argument on the other side. I am wondering how you feel about the following description. As to "smart," they are not smart; a smart contract is just an "if/then" statement. Somebody plugs input into it and something then automatically happens. As to the "contract" part, a smart contract is not necessarily a contract—because it does not necessarily meet the common law standard—offer, acceptance, consideration and all of that kind of stuff. What do you have to say about all that?

Katy Blackwell: I would agree on his take with the contract, it's not really what we call a contract. The smart thing, well yes and no. It's not coming up with this on it's own. But you can tell it to do a number of things and it's going to automatically do them, so in that way I think it is smart in it's own way.

Joan M. Heminway: It is like a little tiny bit of artificial intelligence.

Katy Blackwell: Yeah.