The Computer & Internet Lawyer

Volume 34 ▲ Number 11 ▲ NOVEMBER 2017

Ronald L. Johnston, Arnold & Porter, LLP, Editor-in-Chief

The Risks of Segregated Witness: Problems under Electronic Contract and Evidence Laws

By Jimmy Nguyen

For bitcoin, a critical question is how to increase the network's scalability to achieve the vision of faster transactions and greater usage. That is important to enable the greater "Bitcoin 2.0" vision where bitcoin tokens become not just a widely-used currency, but also fulfill their potential as "programmable money" used to perform technological functions such as smart contracts. The Bitcoin Core development team's proposed scaling solution is Segregated Witness, which would separate signature data (witnesses) from transaction data. (In May 2017, a group of companies supported an agreement for SegWit 2x, which would both implement SegWit and then supposedly later lift the block size from 1MB to 2MB.) Other forces in the bitcoin community believe larger block sizes are the answer, and oppose SegWit as fundamentally changing the nature of bitcoin for little benefit. But in addition to its technical problems, SegWit also could create significant risks under legal systems; by separating and discarding signature data, SegWit

Jimmy Nguyen is Chief Intellectual Property, Communications and Legal Officer for the nChain Group of companies. nChain is the global leader in research and development of innovations in blockchain technology. Mr. Nguyen is an intellectual property and digital technology lawyer who joined nChain after a 21-year legal career in the United States. During his private practice career as a partner in major US law firms, he represented multinational corporates and emerging companies in the technology, entertainment and media, financial services, consumer products and retail sectors. A leader in the legal community, Mr. Nguyen was formerly Chair of the State Bar of California's Intellectual Property Law section, co-chaired the Beverly Hills Bar Association's IP, Internet and New Media section, and co-chaired the California Minority Counsel Program. Mr. Nguyen has been recognized by Lawdragon as one of the 500 Leading Lawyers in America (2008) and a "dynamo talent," by the Century City Bar Association as "Intellectual Property Lawyer of the Year" (2011), by Diversity MBA Magazine" as a "Top 100 Under 50 Diverse Executive Leader" (2015), by the California Minority Counsel Program as an inductee into its "Diversity Leader Hall of Fame" (2015), and by the Association of Media & Entertainment Counsel with its Industry Leader Award (2017). As data protection issues grew increasingly important, Mr. Nguyen also became a Certified Information Privacy Professional/US.

Wolters Kluwer

would make two forms of proof more difficult: (1) legal proof of electronic contracts which could be signed with bitcoin signatures; and (2) evidentiary authentication of blockchain transactions.

These legal issues could create major practical problems in the business world. Ideally, we are moving to a world in which the bitcoin network can power smart contracts and be used for numerous types of data transactions. But in such a world, what happens if companies and consumers cannot easily authenticate and prove those transactions later when there are legal disputes?

How Bitcoin Transactions Operate

Bitcoin is a decentralized cryptocurrency that allows its unit of value (bitcoin) to be sent without trusted intermediaries. Bitcoin transactions are recorded to the blockchain, an immutable ledger that records transactions in groups, added as a block (approximately every 10 minutes) to the chain of prior blocks.

All bitcoin digital signatures are not meant to be electronic contract signatures; however, they originally were set up in a manner that *could* satisfy the requirements of electronic contract signature law if the parties wanted to use them for that purpose.

The original bitcoin white paper by Satoshi Nakamoto defines "an electronic coin" as "a chain of digital signatures. Each owner transfers ownership control of the coin to the next owner by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership."[1] The transaction data conveys the inputs and outputs of coins being spent, and also could carry additional data to be recorded in the bitcoin transaction. For example, Alice is the controller of unspent coins, and digitally signs, using her private key, a transaction to "spend" those coins. Her digital signature confirms she controls the coins and can transfer ownership control to a recipient (Bob) at his bitcoin address.

All bitcoin digital signatures are not meant to be electronic contract signatures; however, they originally were set up in a manner that *could* satisfy the requirements of electronic contract signature law if the parties wanted to use them for that purpose. For example, Alice could sign her bitcoin transaction—or at a more advanced level, a smart contract whose terms are encoded with the transaction data—using her bitcoin digital signature which serves two purposes: (1) to verify the transaction to be sent and validated to the bitcoin network, and *also* (2) to confirm her assent to the transaction or smart contract terms for purposes of electronic contract law.

A normal bitcoin transaction stores both transaction and signature (witness) data together in a block, with the signatures accounting for approximately 60 percent of the data size. As described below, this means bitcoin transactions signatures *could* satisfy e-signature laws, which often require the electronic contract signature to be "attached to or logically associated" with the contract terms (which could, for example, be coded into bitcoin transaction data). It also allows bitcoin transactions to more easily be authenticated for evidentiary purposes.

SegWit Creates Risk by Encouraging Signature Data to be Dropped

How does SegWit change the picture? Rather than directly raising the 1MB block size, SegWit would indirectly increase a block's capacity to store more transactions by separating the signature (witness) data from the transaction data. It then creates two hashes: (1) a "regular" hash of just the transaction data, without the signatures; and (2) a "witness hash" consisting of a hash of both the transaction data and the witness data. How would this data be stored in a block? The bitcoin protocol already uses a Merkle tree (a hierarchical data structure composed of hashes of information) to efficiently store transaction data, and places the Merkle root into the block header of every mined block. SegWit creates a *second* Merkle tree to separately store the witness hashes, but importantly does not require nodes to keep the signature data.

In fact, SegWit assumes that signature data is needed only when transactions are being *validated*, and can thereafter be discarded as unimportant. As described by its original proponent Pieter Wuille, "[t]hese signatures are only needed at time of validation"; SegWit treats "signatures [as] not part of the transaction" its "redesign would allow you to drop this [signature] data."[2] (Mr. Wuille is a co-founder of Blockstream, a blockchain technology company which helps support Bitcoin Core and advocates for SegWit).

Moreover, bitcoin nodes would *not* be required to keep the signature data. "[SegWit] allows you to drop the signatures from relay whenever you are relaying to a node that is not actually doing full-validation at the time. It also allows us to effectively prune this data from history, maybe we're fine with not all nodes in the network actually maintaining these gigabytes of signatures that are buried under years of proof-of-work now."[3] This is a key point because SegWit opens up the likelihood that most bitcoin nodes do not keep the signature data, because it is simply less efficient and costs more to do so. This creates three possible scenarios on the bitcoin network:

1. Some nodes maintain signatures;

2. No nodes maintain signatures;

3. The most likely scenario: The majority of signatures will be discarded.

If most nodes drop the signatures, the blockchain can only reliably serve as a ledger for worldwide business transactions if:

1. Some nodes choose to specialize in storing all signature data. This gives those nodes special weight (as a trusted source) to verify and authenticate bitcoin transactions and signatures. But this is antithetical to the idea of bitcoin as a decentralized, trustless system, with no central authority; or

2. Companies and consumers operating on the blockchain must keep their own copy of transaction records (or their own nodes storing all blockchain transactions with signature data), so they have access to the signature data later if needed for legal proceedings or audits. But this requires massive data duplication and eliminates the efficiencies of using the blockchain as a decentralized ledger.

Consider how this would operate in the world of paper transactions. After parties sign the hard copy of a contract, the signature block is cut off from the body (where the terms are written). The signature block is then converted to an identifier for indexing and that identifier is placed into a filing cabinet with hundreds of other signature identifiers. The actual signature block itself is discarded in most instances. Years later, unless you personally kept the signature block, if you want to prove that you signed (or did not sign) a specific contract, you could find the signature block identifier but you may not be able to retrieve the physical signature block itself. Or you could have to depend on the good graces of a storage facility that has kept all signatures, and that storage facility now gains extra influence as a transaction verifier.

For the bitcoin network, the end result of SegWit would be unreliability. SegWit's option to "drop" signatures will make it more difficult for business and consumers to use bitcoin signatures to also act as electronic contract signatures and to authenticate transaction records.

SegWit's Impact on Electronic Contract Signatures

In 1996, the American Bar Association reviewed the need for electronic signatures to facilitate online transactions. In its Digital Signature Guidelines, it identified two attributes that were key to replicating physical signatures in a digital environment: (1) *Signer authentication*: a digital signature should demonstrate who signed, and it should be difficult to reproduce by an unauthorized party; and (2) *Document/Transaction authentication*: a digital signature should identify what is signed, to make it hard to falsify or alter the signed matter.[4] Most digital signature regimes, including the National Institute of Standards and Technology (NIST) and eIDAS in the European Union, follow similar principles.

Indeed, bitcoin's digital signature method can satisfy these electronic contract signature principles by using the public-private key approach to signing transactions. As noted previously, the original Satoshi Nakamoto bitcoin white paper even defines an electronic coin "as a chain of digital signatures," and explains that a payee can "verify the signatures to verify the chain of ownership."[5] Thus, the entire system relies on the ability of digital signatures to be used to verify both the signer and ownership of the coins being sent. In contrast, SegWit favors transaction authentication over signer authentication, with little thought to the havoc this might cause when transactions are later disputed.

The Federal e-SIGN Act

SegWit could make it very difficult for parties to an electronic contract to later prove its authenticity. In the United States, electronic contracts (and electronic signatures) between businesses and consumers generally are valid under the federal e-SIGN Act.[6] That law defines an "electronic signature"—a more flexible concept than a digital signature such as those used by bitcoin—to be something "*attached to or logically associated with* a contract or other record and executed or adopted by a person with the intent to sign the record."[7] This requirement provides the basis for authenticating that a contract has been signed and authorized by all parties, much like a physical signature block on paper can be used to show later that the parties actually signed the contract. But under SegWit, can it really be said that the electronic signature is "attached to or logically associated with" the transaction data in a manner sufficient to show intent to approve, given the segregated data trees and the possibility for signature data being discarded? Or does SegWit *detach* and *disassociate* the digital signature from the transaction data?

Moreover, the federal e-SIGN Act indicates the legal validity or enforceability of an electronic contract record "*may be denied* if such electronic record is not in a form that is capable of being retained and accurately reproduced for later reference by all parties or persons who are entitled to retain the contract or other record."[8] That is a key provision of the statute—that is, an electronic contract may be *denied* validity or enforceability if it is not kept in a form that can be accurately reproduced later. Yet, as we have seen, SegWit is not concerned with maintaining digital signatures—only with validating transactions as they occur. The SegWit approach creates significant uncertainty as to whether only a hash of signature data can meet the e-SIGN statutory requirements to prove an electronic contract signature.

Under SegWit, a business or consumer wishing to definitely prove an electronic contract signed using a bitcoin digital signature could—at most—re-associate the witness hash with the corresponding transaction data. But if there is no way to recover the digital signature itself, the electronic contract or record may be *denied* legal validity or enforceability under the e-SIGN Act. Digital signatures could be reliably recovered only if some node chose to retain all signature data. Yet a node only has economic incentive to do so if it acts as a commercial archive service, charging fees to retrieve and authenticate full digital signatures. This would create a new form of trusted intermediary needed to verify digital signatures, which is exactly the opposite of bitcoin's decentralized, trustless system.

US State Laws

Similar problems would arise under US state laws. The vast majority of the US states (47, plus the District of Columbia and the US Virgin Islands) have codified a version of the Uniform Electronic Transactions Act (UETA), which also recognizes that electronic transactions are valid. Similar to the federal e-SIGN Act, the UETA defines an electronic signature as an "electronic sound, symbol or process *attached to or logically associated with* a record and executed or adopted by a person with the intent to sign the record."[9] New York's version goes even further to state that an electronic signature is considered to be "attached to or logically associated with an electronic record" if the electronic signature is "linked to the record during transmission and storage."[10] But with SegWit not requiring signature data to be stored, a party seeking to repudiate an electronic contract signed with a bitcoin digital signature might argue that SegWit signatures generally cannot meet this New York definition of an electronic signature.

The question of whether an "electronic sound, symbol or process" is "attached to or logically associated with a record" is often a complicated factual question. For example, in *Young v. Rose*, an Arizona Court of Appeals explained that whether a "thank you" email sent in response to an email with an agreement attached was an "electronic signature" was not clear; it required a review of facts outside the court pleadings and the agreement. SegWit threatens to further complicate this type of factual inquiry about what constitutes a satisfactory "electronic signature" in a world where bitcoin digital signatures may be used to sign contracts.[11]

Arizona law requires that qualifying blockchain technology be "immutable and auditable and provides an uncensored truth." In a SegWit world where signature data is pruned off, will blockchain records truly be auditable and provide an uncensored truth?

Certainly, laws can be updated to address these questions in a world of bitcoin-enabled contracts. For example, in March 2017, the state of Arizona passed legislation (HB 2417) to amend its version of the UETA (the Arizona Electronic Transactions Act) to confirm that electronic signatures, records, or contracts secured through blockchain technology are valid under the state law.[12] It also recognizes that smart contracts are valid. However, the Arizona law requires that qualifying blockchain technology be "immutable and auditable and provides an uncensored truth."[13] In a SegWit world where signature data is pruned off, will blockchain records truly be auditable and provide an uncensored truth? Potentially creating even more uncertainty, the Arizona bill does not address whether transactions, smart contracts, or blockchain signatures must be recorded fully intact (with transaction and signature data together in the block), or if they are no longer presumed valid if signature data is discarded. If SegWit is activated, the validity of such contracts may become unclear under Arizona's new law and other state laws.

Foreign Laws

Outside the United States, these risks of SegWit also would arise under laws of other countries. Across the European Union, electronic signatures are governed by the Electronic Identification Regulation No 910/2014. Like the United States' federal e-SIGN Act and most state laws, the EU Electronic Identification Regulation defines an electronic signature "as data in electronic form which is *attached to or logically associated with* other data in electronic form and which is used by the signatory to sign."[14]

Each EU member country enacts its own laws to implement this EU Regulation. For example, United Kingdom law defines an electronic signature as "so much of anything in electronic form as:

(a) is *incorporated into or otherwise logically associated with* any electronic communication or electronic data; and

(b) purports to be used by the individual creating it to sign."[15]

Therefore, SegWit will create similar issues in the European Union because it allows bitcoin digital signatures to be dropped from transaction data.

China is another important jurisdiction to examine because the bitcoin community—especially for bitcoin mining—remains very strong in the country (despite recent Chinese government action against bitcoin activities). China's Electronic Signature Law defines an electronic signature as "data in electronic form contained in and attached to a data message to be used for identifying the identity of the signatory and for showing that the signatory recognizes what is in the message."[16] Chinese law thus makes explicit that an electronic signature be actually "contained in and attached to" the data message it verifies. This is reinforced by Article 13 of the Chinese law, which deems an electronic signature to a data message to be reliable if it meets four conditions:

1. When the creation data of the electronic signature are used for electronic signature, it belongs to an electronic signatory,
2. When the signature is entered, its creation data are controlled only by the electronic signatory,
3. *After the signature is entered, any alteration made to the electronic signature can be detected*; and
4. *After the signature is entered, any alteration made to the contents and form of a data message can be detected.*[17]

If alterations to the electronic signature or the data message contents occur, they must be detectable. SegWit's alteration of a bitcoin transaction structure can be detected, but may be difficult to reconstruct if nodes do not keep full signature data. This can create risk that a bitcoin digital signature cannot qualify as an electronic signature in China because it is separated from the data message.

SegWit also opens up the very real possibility that some nodes (who save full signature data) could be anointed as more "trusted" to verify transactions and signatures. Indeed, the EU's Electronic Identification Regulation sets out a framework for its member governments to recognize "qualified trust service providers" who are authorized to validate "qualified electronic signatures" so parties can rely upon their validation.[18] Likewise, China's Electronic Signature Law also allows for verification of electronic signatures by a government-approved third-party "electronic verification service."[19] In a SegWit world, nodes who save full signature data would be better positioned to fulfill this service provider role; it means those nodes could become government-authorized validators of what is—or is not—a "qualified electronic signature." That would move bitcoin from a trustless system to one where a centralized authority gains government-approved trust power, a move which would contravene bitcoin's spirit.

Evidence Authentication Issues

Another key legal issue arises under evidence law. Could SegWit make it more difficult to authenticate blockchain-recorded transactions under courtroom evidence laws? In civil and criminal court proceedings, evidence needs be authenticated before it can be admitted. Under US federal evidence rules, "[t]o satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is."[20] This requirement is important to ensure litigants do not try to introduce falsified or tampered evidence.

How does this work in practice? Consider a lawsuit concerning an automobile accident. Drivers often seek to introduce pictures of the accident scene. They could testify from personal knowledge that they used their smartphones to take pictures immediately after the accident and confirm the images are authentic. Similarly, transaction and other business records can be admitted into court proceedings, but a witness typically must testify to authenticate the records. For example, if you are involved in a dispute with your stock exchange over a stock trade, the stock exchange could introduce its electronic records of your account and trades, but one of its employees needs to testify about the authenticity of the data. Likewise, you could produce your own printed copies of your stock trade history and testify about those printouts. Thus, transaction records generally require a witness to explain what the transaction record is, how it is kept or was generated, and what it represents.

How Can Blockchain Receipts Be Authenticated without Signature Data?

How would this work in the blockchain world? If signature data is kept, it is easier to later authenticate the transaction record by referring to the bitcoin digital signature used to validate the transaction. This helps meet the evidentiary requirement that the blockchain record "is what the proponent claims it is"—in other words, the blockchain receipt for the specific transaction.

But SegWit allows signature data to be dropped from the transaction data, making the task of evidentiary authentication more difficult. If all nodes do not maintain signature data, who can testify as to the authenticity of signature data to match it to the relevant transaction data? Although the direct parties to a transaction could hopefully do so, what happens if they relied upon bitcoin nodes to maintain the signature and transaction data and did not keep (or lost) their own records? Would that place nodes who opt to keep full signature data in a special "trusted" position to verify bitcoin transactions for legal proceedings (such as a government-approved service provider, as described previously)? Or would mere evidence that a signature was necessary at the time of the bitcoin transaction satisfy a court, if no such signature can now be produced?

Blockchain advocates need to champion the reliability and immutability of blockchain records. But would legislators be so quick to recognize blockchain records if they knew the basic signature data that has always been saved with bitcoin transaction data could be dropped?

These evidence issues also will play out at the US state level. As more blockchain technology enthusiasm grows, US state legislatures are beginning to examine what is sufficient proof of blockchain business transactions. In 2016, the state of Vermont enacted H.868; it adds a statute to Vermont's Rules of Evidence stating that a blockchain-based digital record is now considered a business record and thus admissible over hearsay objections.[21] One wonders, however, whether other states will follow suit, if SegWit reveals that key components of bitcoin transactions (such as signature data) can be dropped or altered from blockchain records. In order to pass statutes such as the Vermont evidence law, blockchain advocates need to champion the reliability and immutability of blockchain records. But would legislators be so quick to recognize blockchain records if they knew the basic signature data that has always been saved with bitcoin transaction data could be dropped?

Need for a Witness

If signature data is not kept by any bitcoin nodes or only some of them, it creates a serious question of what witness (if any) can adequately authenticate bitcoin transactions from the blockchain. Although it was not dealing with blockchain, the US Court of Appeals for the Ninth Circuit decided an immigration case—*U.S. v. Lizarraga-Tirado*—that addressed questions about the admissibility of machine-generated evidence.[22] The case led James Ching, a *Law.com* contributor, to write a January 2016 blog asking "*Is Blockchain Evidence Inadmissible Hearsay*?"[23] and triggered other online articles questioning whether blockchain evidence is admissible in court.[24] As Ching describes, a blockchain verification "receipt must be introducible in litigation in order to be of any value as a verifier of a transaction. Because a receipt obviously is asserting the existence of the transaction, it must qualify as a business record or it is inadmissible hearsay under the Federal Rules of Evidence."[25] (These blockchain evidence issues were further examined in a June 2017 law review article entitled "Blockchain Receipts: Patentability and Admissibility in Court."[26])

The *Lizarraga* case involved the deportation of a defendant who was found improperly entering (again) the United States through the Mexico border. The defendant claimed he had not actually crossed over the border to the US side. However, the government sought to introduce the evidence of a Google Earth satellite view of the scene where the defendant was arrested, including a tack marker to reflect the border agent's notation (on a mobile device) of where the arrest occurred (on the US side of the border, according to the agent). But that pin marker was manually added to the machine-generated satellite image to record the agent's contemporaneous impressions of where the arrest occurred.

To evaluate the admissibility of the Google Earth map image and the tack marker indicating whether the defendant crossed the US border, the Ninth Circuit decided that machine-generated evidence can be admissible in court (and is not hearsay because it is a machine, rather than a person, making an assertion); however, the evidence still requires that some witness authenticate it. The party offering the machine-generated evidence must show that the "machine is reliable and correctly calibrated, and that the data put into the machine (here, the GPS coordinates) is accurate."[27] The court noted that the rules of evidence allow for authentication of a "process or system" with evidence "describing the process or system and showing that it produces an accurate result." In the case of Google Maps, its satellite mapping and GPS coordinates could be authenticated by a Google employee or other witness who works with the program frequently, if they can testify about how the Google Earth system works. The key is "to establish Google Earth's reliability and accuracy."[28]

How would this authentication requirement be applied to a blockchain receipt offered as evidence in court? A witness would have to testify about the bitcoin network and its "reliability and accuracy" as a mechanism for maintaining business records. The *Blockchain Receipts* law review article noted previously gives examples of what types of witnesses could serve this function to explain the blockchain and its transaction record system: "an exchange programmer, an avid Bitcoin user, a programmer attempting to replicate the blockchain, a digital currency expert, or an investor could all be brought in at trial."[29] That is certainly possible with respect to the original form of bitcoin transactions (which retain both transaction and signature data). But the task is more difficult with SegWit, which allows nodes to drop the signature data, and could lead to complex evidentiary battles about the "reliability and accuracy" of the blockchain-stored data.

Thought Experiments about the Legal Risks

At the 2017 Future of Bitcoin conference in Arnhem, Netherlands, Bitcoin Unlimited's Chief Scientist Peter Rizun gave a presentation about why bitcoins with SegWit are not real bitcoins. To illustrate his point, he offered this thought experiment:

> Imagine that you have 100 BTC in a segwit address and a few days later you notice that they've been transferred to an address that you do NOT control. You try to find the signature that authorized the transfer to prove the theft (you're sure your private keys were secure so you think the signature must be bogus) but conveniently nobody seems to have it saved.
>
> Can you prove that your funds were stolen?[30]

In Rizun's thought experiment, assume you sue your bitcoin wallet provider over the 100 BTC that you believe were stolen from your wallet. As Rizun points out, you need to find the signature associated with the transaction in order to prove it was fake and not authorized by you. But, of course, you would not have kept it because you did not initiate the transaction. And if your wallet provider and no node has kept the signature for the disputed transaction, you are out of luck. At most, you or your wallet provider may only be able prove: (a) a transaction occurred on a particular date and time for the 100 BTC; and (b) there is a string of hashes that indicate that transaction was authorized at that time. Is that enough to authenticate that transaction record for evidence purposes? And more importantly, even if that limited transaction record is authenticated and admissible in court, the signature data is missing and a key question in the case cannot be answered from the evidence.

Law is very slow to catch up with transformative technology and SegWit makes the challenges harder.

Take Peter Rizun's example a step further with this thought experiment based upon potential smart contracts that could be recorded on the blockchain and electronically signed by one party using a bitcoin digital signature:

> Alice enters into a smart contract to pay you 5 BTC to buy your used automobile. The contract's terms are recorded on the blockchain as part of a transaction by sending the 5 BTC to a SegWit address. Alice's digital signature to validate the bitcoin transaction is also the means Alice uses to digitally sign to signify acceptance of the smart contract (for purposes of e-contract law). [In other words, Alice does not manually sign a paper contract, does not affix a digital copy of her handwritten signature to any document, and does not electronically sign a document using other means.]
>
> Alice later disputes the smart contract, claiming that she did not authorize the transaction. You have a legal dispute over whether she in fact digitally signed the smart contract. But Alice's signature data was pruned after the transaction was validated onto the blockchain, and she claims she did not digitally sign the transaction. You have no record of Alice's private key used for the digital signature.
>
> Can you prove that Alice digitally signed the smart contract?

This thought experiment illustrates the potential proof challenges of a SegWit world. It can be more difficult to prove that Alice digitally signed the disputed smart contract if you have no record of Alice's private key used for the digital signature, and no node has kept the signature data.

Can legal systems in the United States and other countries solve these problems? That is always possible, but law is very slow to catch up with transformative technology and SegWit makes the challenges harder.

In a SegWit world, signature data may not always be "attached to or logically associated" later with transaction data. That would contravene the leading legal framework for electronic contracts and trigger additional hurdles for authenticating blockchain records as evidence in legal proceedings. These risks could deter businesses from operating more on the blockchain, and impede the greater vision of a Bitcoin 2.0 network powering smart contracts and greater functionality in the future. To achieve greater Bitcoin 2.0 vision, the bitcoin community needs to demonstrate to businesses, courts, regulators, and legislators that bitcoin records—and in particular, signatures—are reliable and authentic; this effort is just getting started and should not be undermined by proposals such as SegWit which fundamentally change the nature of bitcoin.

Notes

1. Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (2008), available at *http://bitcoin.org/bitcoin.pdf*.
2. "Bitcoin scalability with SegWit," speech by Pieter Wuille on December 6, 2015, at Scaling Bitcoin conference, Hong Kong. Transcript available at *https://diyhpl.us/wiki/transcripts/scalingbitcoin/hong-kong/segregated-witness-and-its-impact-on-scalability/*; video available at *https://www.youtube.com/watch?v=fst1IK_mrng&t=36m*.
3. *Id*.
4. "Digital Signature Guidelines," Information Security Committee, Electronic Commerce and Information Technology Division, Section of Science and Technology, American Bar Association, August 1, 1996, pp. 7-8.
5. Nakamoto, S., (2008a) "Bitcoin: A Peer-toPeer Electronic Cash System," available at *http://bitcoin.org/bitcoin.pdf*.
6. 15 U.S.C. Code § 7001.
7. 15 U.S.C. §7006(5).
8. 17 U.S.C. §7001(e).
9. Uniform Electronic Transactions Act (1999), section 2(8) (emphasis added).
10. 9 CRR-NY 540.4(b).
11. Young v. Rose, 286 P.3d 518 (Az. App. 2012).
12. Arizona HB 2417 (2017).
13. *Id*.
14. Regulation (EU) No 910/2014 of the European Parliament and of the council, July 23, 2014, Article 3(10) (emphasis added).
15. United Kingdom Electronic Communications Act 2000, section 7(2) (emphasis added).
16. Electronic Signature Law of the People's Republic of China, Article 2 (emphasis added). *See* WIPO English translation available at *http://www.wipo.int/wipolex/en/text.jsp?file_id=182409*.
17. *Id.,* Article 13.
18. EU Regulation No. 910/2014, Article 33(1).
19. Electronic Signature Law of the PRC, Articles 16-18.
20. Fed. R. Evid. 901.
21. 12 Vermont Statutes Annotated § 1913.
22. U.S. v. Lizarraga-Tirado, 789 F.3d 1107 (9th Cir. 2015).
23. James Ching, "Is Blockchain Evidence Inadmissible Hearsay?," *Law.com*, January 7, 2016, available at *http://www.law.com/sites/jamesching/2016/01/07/is-blockchain-evidence-inadmissible-hearsay/*.
24. Casey Sullivan, "Could Blockchain Evidence Be Inadmissible?," *FindLaw.com*, May 5, 2016, available at *http://blogs.findlaw.com/technologist/2016/05/could-blockchain-evidence-be-inadmissible.html*; Lester Coleman, "Blockchain Receipts: Admissible as Evidence or 'Hearsay?," *CryptocoinsNew.com*, August 1, 2016, available at *https://www.cryptocoinsnews.com/blockchain-receipts-admissible-evidence-hearsay/*.
25. James Ching, "Is Blockchain Evidence Inadmissible Hearsay?," *Law.com*, January 7, 2016.
26. Angela Guo, "Blockchain Receipts: Patentability and Admissibility in Court," *Chicago-Kent Journal of Intellectual Property*, Vol 16, Issue 2, p. 440 (June 21, 2017), available at *http://scholarship.kentlaw.iit.edu/cgi/viewcontent.cgi?article=1185&context=ckjip*.
27. *Lizarrage-Tirado,* 789 F.3d at 1110.
28. *Id*.
29. *Guo*, at 447-448.
30. "SegWit Coins are not Bitcoins," presentation by Dr. Peter Rizun, The Future of Bitcoin conference, June 30, 2017 (Arnhem, Netherlands). Video available at *https://www.youtube.com/watch?v=VoFb3mcxluY*.

Reprinted from *The Computer & Internet Lawyer*, November 2017, Volume 34, Number 11,
pages 1–8, with permission from Wolters Kluwer, New York, NY,
1-800-638-8437, *www.WoltersKluwerLR.com*.