
ACC DOCKET

INFORMED. INDISPENSABLE. IN-HOUSE.

Add Value to Your Company's Blockchain Initiative as a Cross-Functional Advocate

Technology, Privacy, and eCommerce



CHEAT SHEET

- **Lead the way.** In-house counsel have a unique opportunity to shape, frame, and design contractual partnerships, as well as share knowledge and information across the C-suite

regarding blockchain initiatives.

- **Help the top.** When talking to your CEO about blockchain, give them the big picture, disruptive risks, and potential opportunities, focusing on Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis.
- **Learn from the master.** Engage your chief information security officer on critical security components to using blockchain. Develop suggested policy leadership positions, and come prepared with case studies of blockchain as the subject of cyberattacks.
- **Privacy matters.** When working with the chief privacy officer, emphasize the need for compliance, and strategize a long-term plan for managing privacy regulations if the blockchain extends beyond a pilot phase.

If your company has recently embarked on a blockchain pilot program, you have an important role to play as in-house counsel. Not only do you need to work with the project managers to engage the consultants and engineers who will be essential for delivery, but also other partners, suppliers, customers, and vendors. As you help shape, frame, and design these contractual partnerships, your unique horizontal view across this important initiative means you are positioned to identify and manage the myriad risks, but also help share knowledge and information. You can add value by being an advocate across the C-suite to think strategically and stay apprised of important opportunities that impact the blockchain initiative.

If you need a primer on blockchain, ACC has many resources (check out the Extras on page 66). As a quick reminder, blockchain is a new type of database technology that uses smart contracts and distributed systems to reduce time and processes (i.e., costs) and improve security and transparency. It could be as revolutionary as the internet itself as it begins to connect companies, suppliers, and customers across a new networked system that will better meet future needs.

To help you be prepared for what type of regulation and policy could be needed, and to advise your C-suite executives, it's helpful to look historically at other similar shifts. Because blockchain is a protocol for connecting a group of decentralized computers, it is similar to how the internet was developed and rolled out. Some actually believe blockchain could replace how we connect computers to the internet, or it could be an alternative to the existing domain name infrastructure that creates the internet in the future.

To function on the internet, a computer must have some basic information, such as its IP address and the IP address of at least one router and a few critical services.

As the domain name system (DNS) became standardized in the 1980s and 1990s, another important and related trend was occurring. According to the Current Population Survey (conducted by the US Census Bureau), personal computer adoption in the United States continued to increase throughout the 1990s and demonstrated a fivefold increase from 1984. According to Internet World Stats, by 2000, 5.8 percent of the global population had a computer with access to the internet. In the United States, by the year 2000, 51 percent, or 54 million households, had access to at least one computer at home, up from 36.6 percent in 1997. The percentage of households with internet access more than doubled between these years, from 18 percent in 1997 to 41.5 percent, or 42 million households, by the year 2000. Computer access and internet access were becoming synonymous: More than four in five households with computer access also had internet access.

Sometime around 1996 or 1997, browser manufacturers made dotcom the default value for any names typed directly into the browser command line. That is, whenever a user typed without a top-level domain into the command line, the browser automatically directed the user to *www.<name>.com*. Making dot-com the default value for all browser entries reinforced the value of dot-com registrations relative to other top-level domains (i.e., *dot.org*, *dot.net*, etc). In effect, a dot.com domain name functioned as a global keyword, and the possession of a common, simple word in the dot.com space was sure to generate significant traffic from web browsers.

As blockchain evolves, we must watch for how consumer adoption of the concept and/or adoption of new blockchain based assets of value is driven by the companies developing the tools, devices, and interface with which we access this new underlying technology.

For example, will our desire for privacy and security, combined with the rapidly evolving Internet of Things and artificial intelligence technology, mean that some form of blockchain will become a default setting of purchases? Or will one blockchain platform earn our trust as consumers more than another, so we want to know what brand of blockchain is inside the devices that connect our life?

Not surprisingly, as the underlying technology and protocols governing the internet connected the world commercially, industries were adapting and changing at the same time. Consider how the financial sector exploded with the advent of electronic trading, and the ability to manage personal account finances, stocks, and accounting online. This led to a revolution in the financial industry as it turned into a 24/7 operation, with market reactions often being instantly impacted by algorithms or fear, and by humans with the ability to transact their own business online immediately.

Likewise, big telecommunications companies identified the new network infrastructure that was required. Verizon, AT&T, Time Warner, Comcast, and others invested billions in the last mile of deploying broadband and connectivity. New infrastructure, like cellphone towers, changed the landscape. Today's debate over net neutrality questions whether those companies that invested in that infrastructure should now be regulated and required to provide equal access, or whether they should be able to charge what the market will bear from the companies pumping out content using their bandwidth.

What similar investments are being made today to power the blockchain revolution that could later be regulated? What infrastructure is needed to scale blockchain? What standards and norms will be needed to connect a group of decentralized computers and then provide consumers access to it in some trusted way? What investments are needed for blockchain to transform our world? If you are considering how blockchain will affect your business, don't underestimate this comparison — think about the possibilities at a deeper level. As a cross-functional advisor, you can help your executive colleagues be prepared to think about these opportunities and develop a policy and regulatory strategy to position your company for the greatest success in the future.

ICANN, the governing body of the internet, was formed 21 years ago. It took about 10 years for the revolution to fully take shape, so even in recent examples, we are seeing a long window for transformation. We are at similar crossroads in blockchain. Do you want to wait and let others lead the transformation, or do you want to take part in it? What lessons can we learn from prior failures?

As you consider these examples of how a technology or concept was developed and what steps were taken to standardize it and create the products, software, and network required to leverage its power, we can derive predictions about what could happen with blockchain. Blockchain will not be something a consumer buys, but they will come to recognize it as something they trust, like the

branded “Intel Inside.”

Companies that will make money from the blockchain investment are not unlike the early development of Verizon, Time Warner, Comcast, and others that have evolved during the internet age. Some type of connectivity is going to be required — what system will that be? Is it something that already exists or can connect to, or will an entirely new system be needed?

Some type of centralization of blockchain protocols will be required. If that is developed, could it be scaled and licensed to users? As blockchain develops, there are tremendous areas of opportunity alongside the risks. As you consider your role in the standardization, carefully evaluate the opportunities that exist for your business — it could change everything. Where will your company fit in this matrix?

Here's how you can work most effectively with key C-suite executives.

Chief executive officer

Your CEO is most interested in assessing disruptive risks and opportunities that drive strategy for your organization. CEOs need to be able to make reasonable assumptions about the future landscape to suggest investment decisions that can pay off for the shareholders of the company. Accordingly, when it comes to blockchain, you can help frame this in the context of other historical shifts and where your company fits into the potential blockchain revolution.

Leverage the knowledge you obtain from developing the strategic partnerships and researching what predictions your vendor partners have along with an analysis of what your competitors are doing. If you can help your CEO develop a set of assumptions about blockchain, then you can help your CEO make smart decisions about when and how to invest in this area.

Remember that when talking with your CEO, they don't want the “lawyer's” analysis of risk, they want advice on how this could disrupt the entire business model. They also don't just want the downside risk. They want to know: What is the upside? If your company takes a leadership role, how could that position you to deliver your product or service? Most CEOs appreciate a simple SWOT analysis of any issues. What are your strengths and weaknesses when it comes to blockchain, and what are the opportunities and threats? Frame this in the context of your competitors, and you can help your CEO determine what resources to apply to the initiative. Utilizing the development of the internet as a point of reference is helpful because it's a recent paradigm shift most CEOs experienced first-hand, so it can help your CEO grasp the mistakes companies made during that revolution and avoid the same mistakes.

What's important to the CEO?

- Big picture, disruptive risks, and opportunities;
- Assumptions about the future to make investment decisions; and
- Competitive analysis and macro trends.

How legal can help

- Focus and frame the information obtained from vendor partners into a summary of recommendations on what's important about the future of blockchain for your organization.

-
- Don't focus just on the down-side, look for opportunities for the company to make money (through revenue or cost savings), and be a leader in the future.
 - Summarize what competitors are doing and have a point of view about where your organization fits in that matrix.

Chief information security officer

Blockchain, in theory, will be more secure than other existing centralized databases. Take time to discuss some of the critical security components to using blockchain with your chief information security officer (CISO). Offer to be an oversight partner pilot programs are rolled out. First, consider that blockchain will be heavily built using open-source code. At the very outset, you can help put in place an open source compliance program that will include tracking usage, vulnerabilities, and patches. This is absolutely critical to ever achieving the goal of greater security. If your CISO is not already engaged in an open-source compliance program, this is a great opportunity to help not only in blockchain but potentially in other initiatives. Some organizations have centralized open-source tracking, others may be done by department. Your CISO may appreciate the opportunity to centralize this function with your help. You can also work with your CISO to evaluate security vulnerabilities holistically with the project management team.

As you approach working with your CISO (and the engineers for that matter), be sure to understand the real security components of blockchain. Start by understanding how blockchain has been used in the cryptocurrency world to try to evade hackers or "bad actors."

Many proponents of blockchain believe that it is able to overcome the "bad actor" in humans and prevent humans from hacking into the system. No matter how good the technology, humans are always part of the equation. Let's take the example of the Decentralized Autonomous Organization (DAO, a digital currency exchange) infamous hack of blockchain technology.

Some governing body or structure with a clear set of rules and accountability will be required for people to trust clearinghouses for transactions and property.

In the case of DAO, hackers made off with US\$50 million in virtual currency. DAO was supposed to be a way of decentralizing an investment fund. Instead of a few partners deciding which companies to invest in, the members of the fund made the decisions.

The more you contributed, the more weight your vote carried. The distributed nature of the fund meant no one could run off with the money.

DAO is built on the Ethereum blockchain platform. The idea was to have more democracy in the financial institution. Each unit of Ether (the currency of Ethereum) is unique and traceable. DAO says if the hacker tries to sell the stolen Ether, the system will flag it. It turns out, though, there may have been a mistake in the code that allowed a hacker to run a transaction, withdrawing funds before the system realized it was happening. Through that weakness in the code, the hacker was able to steal millions of "dollars" in Ether. As explained in Wired magazine, the DAO team could solve the problem simply by recreating what existed before the hack, ostensibly turning back the clock to before the hack.

This, however, raises the very concerns that so many have about cryptocurrencies and blockchain in general. If it can all be rigged and manipulated like this, how can anyone trust it? Doesn't that create

a bigger problem than the technology is trying to solve?

This conundrum, like many others, will have to be solved for blockchain to truly transform our world as its proponents claim it can. Wherever this kind of manipulation can occur, rules and governance principles will be needed.

Imagine, for example, if a county recorder's office could simply turn back the clock on real estate transactions and undo the sale of a building or a home because someone of great influence wanted it. How could anyone rely on this as a clearinghouse for transactions of such importance? Some governing body or structure with a clear set of rules and accountability will be required for people to trust clearinghouses for transactions and property.

As the technology develops further, the question of what type of governance is required undoubtedly will equally evolve. Many companies and groups are attempting to solve this problem. The list is too long to even begin to cover — IBM is prominently in this space, but many universities and academics around the world are also jumping into the discussion, along with the big consulting companies like Deloitte, E&Y, and PWC vying for a seat at the table as these new governing principles are developed. Additionally, the organizations that traditionally lead the formation of standards like the ISO are forming committees to address this issue.

There are probably hundreds, if not thousands, of groups discussing and trying to form governance-based solutions to this question right now. But how will anyone government, let alone the world, agree upon a single standard or framework? How will these complex issues be resolved? Will the industry that has quickly formed around it backed by big companies self-regulate and create it? Will an intergovernmental organization like ICANN form to create a stakeholder-based model? Or will the marketplace weed out the weak companies and ideas in favor of a predominant, scalable model? Will you be a part of the discussion or just wait and see what happens? These are all discussion points to raise with your CISO.

What's important to the CISO?

- Managing vulnerabilities created by rolling out a blockchain;
- Finding long-term strategies to minimize cyberattacks; and
- Controlling costs on projects that may be distracting from what they view as more contemporary threats. Blockchain may not be something they want at this time.

How legal can help

- Develop suggested policy leadership positions to manage risk associated with blockchain.
- Come prepared with case studies of cyberattacks on blockchains and the steps outlined to minimize the risk of it happening to yours.
- Develop your own viewpoint on the return on investment of the blockchain project as it relates to long-term security benefits to the company.

Chief marketing officer

The next C-suite officer on your meeting list should be your chief marketing officer (CMO) or chief digital officer, depending on how your company is structured. The most important legal component to meeting with the CMO is to understand how the CMO may want to market your company's use of

blockchain in the future.

Most blockchain is built using open-source code, but some components of what you develop could be patentable. As referenced above when talking with your CISO, an open source code policy is essential. Depending on what your company wants to market, you may want to consider a strategic patent program to identify design patents for any user interface that's developed, as well as traditional patents to protect underlying components of what is developed that could be proprietary and marketable for your company.

Work closely with your IP advisors to understand what can and can't be protected, but first understand how the company plans to market its use of blockchain. All too often, we think of patenting as something you do after the development stage, but to effectively develop, use, and leverage patents, it really needs to be the other way around. What would you market, and sell that would benefit from being proprietary — then go work with the engineers to build that and protect it from the outset. This is an important distinction from how most companies currently manage patents. With blockchain's heavy reliance on open source code, it's absolutely essential to work with your CMO to understand how the company may market its blockchain initiative to know what should and shouldn't be patented.

What's important to the CMO?

- How the company might market to new audiences through the use of blockchain or cryptocurrency;
- What competitors are doing and how they can differentiate the company; and
- New product or service offerings using blockchain.

How legal can help

- Utilize patent analytics to help the CMO know what competitors may offer that is unique or proprietary in the future;
- Leverage vendor and partner relationships for research about future product and service offerings; and
- Frame the conversation focused not on risks, but on opportunities for the company to differentiate itself through its use of blockchain.

Chief privacy officer

Many companies now have a chief privacy officer (CPO), though some continue to manage privacy within the legal group. As you work with your CLO and/or CPO, in addition to keeping them apprised of all of the work you are doing with the C-suite team, you can specifically help them consider the risks to the organization as blockchain is rolled out.

If it is a true public blockchain then careful attention must be paid to what information can be seen or viewed by all members of the blockchain. If it is semi-private or private, then safeguards must be in place to ensure the connecting of the computer through the blockchain is compliant with a now rapidly changing privacy landscape.

One of the most important components of blockchain is that it is “transparent.” If it is a true public

blockchain then careful attention must be paid to what information can be seen or viewed by all members of the blockchain. If it is semi-private or private, then safeguards must be in place to ensure the connecting of the computers through the blockchain is compliant with a now rapidly changing privacy landscape.

The European Union's major privacy legislation, the General Data Protection Regulation (GDPR), for example, is immediately triggered through the use of a blockchain. This requires user agreements that understand the nature of what information is transmitted and available across the blockchain. Accordingly, a compliance program is immediately required to ensure that even in a test case or pilot program that the use of the blockchain complies with GDPR. This is why many test programs are very narrow in nature and carefully framed through contracts to avoid triggering any privacy legislation. However, if the project is to expand and scale, inherently, it means that private information will be managed through the blockchain. While it may not be triggered in the pilot program, start working with your CPO, and think through a long-term plan for managing privacy regulations if the blockchain goes beyond a pilot phase.

What's important to the CLO/CPO?

- Compliance with the myriad of privacy, open source, and other regulation that is known and unknown;
- Understanding when and how legislation and or regulation will impact blockchain initiatives; and
- As budgets remain tight, allocating precious resources to a test project may not be top on the list.

How legal can help

- Stay apprised of all new developments related to blockchain regulation. This means following government regulatory agencies and tracking any legislation that may tangentially deal with blockchain.
- Follow the big open source projects like Ethereum and Hyperledger to know when legal issues are being discussed. Set up alerts for blockchain to know when new legislation is being proposed.
- Track the value that is being added to the organization through the work you are doing with blockchain so you can help your senior leaders make the business case to allocate time, money, and resources (including your time) when needed.

Chief information officer

Most likely, the project will reside within the chief information officer (CIO) function (though that can depend upon the company). As you assist the CIO in managing the project for the organization, there are a few key questions to discuss here.

- From an operational perspective, what are the benchmarks that will determine whether or not blockchain is rolled out beyond a test program?
- How could blockchain replace legacy systems? If so, when and how would that happen?
- As regulation is developed, what is the company's appetite to help set and shape those policies and regulations?

You have an important role as in-house counsel to understand the questions and the answers to these key questions so you can manage not just the contracts, but the overall legal strategy in how blockchain is tested and ultimately rolled out. If you don't have a key grasp of these issues, you can't put in place a strategy to achieve those outcomes:

- Replacing legacy systems;
- Introducing new products or services;
- Accepting new forms of currency;
- Using existing blockchain platforms versus building your own; and
- Connecting the blockchain to the end user.

As counsel, you will help shape the future of your company's role in the blockchain age. Consider the profound impact you can have by cross-functionally advising your senior leadership:

- Framing and forming strong contractual partner relationships;
- Developing policy and advocacy for regulation that will position your company for the future;
- Developing strategic intellectual property for marketing initiatives; and
- Verifying the security of the blockchain by managing open source code effectively.

What's important to the CIO?

- Achieving project goals to evaluate if the blockchain project will go forward. The CIO needs to justify the time, money, and resources;
- Understanding the long-term opportunities to the organization to evaluate if more investment should be deployed; and
- Getting it done. They don't want to have things delayed in legal.

How legal can help

- Work closely with your CIO or project managers to understand their benchmarks of success and goals. Be a partner and not a roadblock.
- Frame and create partnership agreements tailored to the business goals. Be flexible on contractual terms to achieve business goals so long as there are clear renewal points to renegotiate as it evolves from a pilot to a larger scale program.
- Ask to attend regular operations meetings and add value by understanding the opportunities and key questions to ask.

In-house counsel have a unique view into all of these areas because they touch all facets of the agreements that put in place the infrastructure. Rather than responding to the proverbial "in-box," take a lead in advocating for opportunities in your organization by understanding what's coming in blockchain and bridging gaps between functions.

ACC EXTRAS ON... Blockchain

Articles

[Quick Overview: Blockchain Basics for In-house Counsel \(April 2019\).](#)

[Global Legal Insights — Blockchain & Cryptocurrency Regulation 2019, 1st Edition \(Sept. 2018\).](#)

Sample Forms, Policies, and Contracts

[Getting a Voice on the Blockchain: “Delegated Proof of Stake” Interesting for Companies \(Aug. 2018\).](#)

Jennifer Wolfe



CEO

Dot Brand 360

Jennifer Wolfe is the author of *Blockchain in the Boardroom*, *Digital in the Boardroom*, *Domain Names Rewired*, and *Brand Rewired*. She is a faculty member for the National Association of Corporate Directors on the topics of digital disruption, emerging technologies, cybersecurity, and the future of work, as well as an accomplished intellectual property attorney.