BARNES & THORNBURG LLP

MEDIA MENTIONS

Blockchain Consortia: A Legal Roadmap To A Dynamically Changing Regulatory Landscape In The US And The EU

Many have predicted that blockchain technology will disrupt traditional commerce across the globe. From global financial and supply chain systems to national…

May 1, 2019 | Chicago

Many have predicted that blockchain technology will disrupt traditional commerce across the globe. From global financial and supply chain systems to national healthcare and insurance industries and on to selling renewable energy from one's roof to their neighbors, this new technology creates a digital, reliable source of truth.

Various distinctions and categorizations of blockchains are used depending on the purpose of the technology. Generally, blockchains are divided into private (permissioned) and public (permission-less) networks. Probably the most known example of a public blockchain is bitcoin, a digital currency that over the last few years has drawn as much excitement as it has disappointment. While the public-at-large continues to seek to profit from trading bitcoin or other cryptocurrencies, companies around the world are attempting to utilize the technology itself to streamline their operations, cut costs, and attract new partners and reach new markets.

One manifestation of the latter type of effort is a so-called "blockchain consortium," a business-to-business initiative that gathers market participants around a common challenge. In such a consortium, each

RELATED PRACTICE AREAS

Intellectual Property

participant contributes its resources to construct and govern a blockchain network. This joint-venture model, while it gives hope for broader utilization of blockchain, nevertheless raises concerns and legal risks that only escalate when consortia operate across geographical borders and legal jurisdictions.

This article discusses these risks and outlines a legal roadmap for a company seeking to participate in a blockchain consortium. Further, the article examines recent developments in the United States and the European Union (EU), specifically highlighting Poland's fast track to becoming a hub for European innovation and a playground for some of the most engaging implementations of permissioned blockchains.

The Legislative Landscape

Over the past few years, blockchain regulatory and legislative activities in the United States have primarily been concentrated around cryptoassets. Some of these activities originate from federal regulators giving guidance about or bringing enforcement actions to address Initial Coin Offering (ICO) issuers and crypto exchanges. But Congress has not taken any concrete steps to legislate blockchain technology in its nascent stages. State lawmakers, on the other hand, including legislators in Arizona, Tennessee, Nevada, Delaware, Ohio, and Wyoming, have passed a variety of laws and empowered state regulation of blockchain technology—all while hoping to attract investors in the crypto and blockchain spaces. Some of these laws cover a broad spectrum of initiatives, while others are directed at recognizing and ensuring the binding effects of blockchain and other blockchain-associated instruments and tools (e.g., smart contracts). At the same time, certain public institutions are already taking concrete steps to implement the blockchain technology into their affairs. For instance, the Cook County Recorder of Deeds in Chicago is collaborating with technology companies to digitalize Illinois properties on blockchain so that sale and recordation processes are more secure and transparent.

In the United States, federal laws and regulations related to securities, commodities, tax, and anti-money laundering requirements, coupled with unharmonized state laws and a mosaic of federal and state currency transmission regulations, create a legal landscape that is highly complex. This complexity causes uncertainty among blockchain participants and, potentially, slowing innovation. But, despite such uncertainty, U.S. companies actively research the applicability of permissioned blockchains in the supply chain, finance and banking, insurance, and healthcare industries.

In the EU, in stark contrast, since the birth of the cryptocurrency industry, the regulators and lawmakers have been closely watching the developments in the blockchain space and responding to these advances by taking numerous legislative actions. For instance, in 2018, the European Commission (EC) launched the EU Blockchain Observatory and Forum, a multilevel platform for discussion on blockchain's developments, impacts, and regulatory challenges. Another step was taken in April 2018 when a group of member states established the European Blockchain Partnership (EBP) and the European Blockchain Services Infrastructure (EBSI) initiatives aimed at supporting the delivery of cross-border digital public services. The EBP continues to grow, with

Hungary joining in February 2019 and becoming the group's 29th member.

Furthermore, on December 13, 2018, the European Parliament (EP) enacted the "Blockchain: a forward-looking trade policy" (2018/2085(INI)) resolution, in which it outlined ways to improve the EU trade policies through the use of blockchain. The EP has also indicated the need to develop "global interoperability standards" to enable cross-blockchain transactions for smoother supply chain processes.

Among the EU member states, Poland is in the lead dynamically developing enterprise blockchain projects. For instance, the recently launched eVoting platform permits investors to participate in online votings of public companies while the Blockchain Based Durable Medium—an electronic regulation document delivery system for the financial and insurance industries—allows the fulfillment of certain legal obligations related to the delivery of client communication. In addition to private initiatives, the enterprise blockchain in Poland is also supported by governmental institutions. The Polish Ministry of Digitization has recently launched a Working Group dedicated to Distributed Ledger Technologies (DLT) and blockchains that focuses on creating a legal framework for the blockchain technology.

As the legal climate around blockchain continues to be supportive, similarly to their U.S. counterparts, EU companies are likely to vigorously pursue the suitability of permissioned blockchains to their economic and operational objectives.

Antitrust

A permissioned blockchain developed or operated by a consortium across national borders likely will be subject to antitrust laws of multiple jurisdictions, including the United States, the EU, and specific EU member states. Pursuant to both the U.S. and EU laws, any collusive or exclusionary blockchain development—such as sharing pricing information in a blockchain developed for use in a specific industry—may violate antitrust laws. Although antitrust regulators have not developed a comprehensive approach to such issues, some guidance exists for anyone seeking to develop and operate a permissioned blockchain.

In 2018, for example, the U.S. Federal Trade Commission (FTC), created an internal FTC Blockchain Working Group to build on its expertise in cryptocurrency and blockchain technology. The Working Group intends to broaden its internal expertise, share resources, and facilitate internal communication and external coordination on enforcement actions. In the area of trade competition, the FTC noted that "[c]ryptocurrency and blockchain technologies could disrupt existing industries. In disruptive scenarios, incumbent companies may sometimes seek to hobble potential competitors through regulatory burdens. The FTC's competition advocacy work could help ensure that competition, not regulation, determines what products will be available in the marketplace." Although to date neither the United States nor the EU has brought an antitrust action against a blockchain network participant, a consortium that uses a blockchain —either inadvertently or purposefully—to share anticompetitive information could face such an action.

In the United States, a claim could be brought under the Sherman

Antitrust Act. Pursuant to Sections 1 and 2 of the Act, market participants are prohibited from unfairly excluding competitors from the use of technologies that are essential to the competitors' business, among other exclusitory conducts. Additionally, the blockchain participants may face enforcement actions under other federal laws, including the Federal Trade Commission Act or the Clayton Antitrust Act.

In the EU, the impermissible activities of blockchain participants may be subject to both the EU and their own country's national-level regulations. For instance, pursuant to Section 6 of the Polish Competition and Consumer Protection Act, any agreement which seeks to or results in eliminating, restricting or otherwise distorting competition, in particular by limiting or controlling technological progress or restricting market access, may be invalidated.

To lower the risk of an antitrust investigation, whether in the United States or Europe, blockchain participants should outline clearly defined and transparent principles as to who may participate in a consortium and on what conditions. The founders of any such consortium ought to consider setting out the rules and principles pertaining to functioning, governance, and decision-making on permissioned blockchains in a contract between participants. Such blockchain governance would serve as evidence that the consortium members had set up substantive and procedural safeguards to ensure against collusive or anti-competitive behavior in or through their blockchain.

Intellectual Property

In any permissioned blockchain consortium, members and participants would be wise to ensure that they have properly protected any intellectual property they have brought to the collaboration, as well as the intellectual property created by or from the collaboration. Regardless of the jurisdiction in which such a consortium expects to operate, consortium founders should give thought to the ownership structure of any blockchain. For instance, founders should consider whether to establish a separate joint venture entity to hold intellectual property rights or to allocate ownership to one of the parties while licensing the intellectual property to other participants. Or, founders may choose to allocate ownership that is pertinent to certain inventions to one participant while vesting the rights to further inventions to others. Alternatively, they may decide jointly to own the inventions related to permissioned blockchains. Because various jurisdictions regulate the exploitation of a jointly owned property this model can be cumbersome. Consortium founders also should give thought to the intellectual property protections available to them to the maximum extent possible.

Smart Contracts

Generally, blockchain networks act as decentralized databases (books of records) storing histories of transactions on a given subject. They can also be used as decentralized virtual machines that execute pieces of code in response to the occurrence of certain conditions. These so-called "smart contracts" are self-executing computer scripts that enable market participants to conduct financial transactions without the need for third-party brokers. While smart contracts could significantly enhance the functionalities of a blockchain consortium, they can also potentially

become the cause for the uncertainty around fundamental contract law concepts related to contract formation, enforcement, and dispute resolution, among others.

From the perspective of U.S. law, the lack of a federal statute regulating blockchain combined with the legislative activities by individual states contributes to uncertainty around smart contracts. At the same time, the Chamber of Digital Commerce, believe that no new laws are necessary because the existing federal framework already "supports the formation and enforceability of smart contracts under state law." Particularly, the framework enables that the Electronic Signatures in Global and National Commerce Act (ESIGN Act) and the Uniform Electronic Transaction Act (UETA) "provide sufficient legal basis for smart contracts executing terms of a legal contract." Lastly, the existing framework states that "[a]dditional state legislation, inconsistently drafted, will confuse the marketplace and potentially hinder innovation."

In both the United States and the EU, the lack of broader statutes contributes to the ambiguity of whether smart contracts are legal contracts at all. Although equipped with new functionalities, smart contracts are similar to the existing means of electronic communication. Pursuant to the EU requirements, to create a legally binding contract, two parties must reach consensus expressed in two consistent statements of will. If parties use a smart contract in a manner sufficient to express one's will, such a smart contract may be recognized as a legally binding contract. That said, numerous statutes require additional forms of reaching and expressing consensus (e.g., a notarial deed in real estate transactions). In such cases, executing a smart contract on blockchain may not be sufficient to create a legally binding agreement. It is also worth noting that EU member countries may have different legal requirements regarding particular branches of law, in those case, for smart contracts to be legal contracts, new enabling legislation may be required in the future.

Also in the United States, market participants may face similar obstacles related to the validity and enforceability of smart contracts. Indeed, regulating smart contracts in one U.S. jurisdiction, but not others, creates even more questions for a consortium that hopes to deploy its blockchain platform across multiple U.S. states. What if one party to a smart contract is domiciled, headquartered, or conducts business from a jurisdiction that regulates smart contracts and the other is not, or if all jurisdictions involved regulated smart contracts, but define certain concepts inconsistently? Indeed, consortia must pay close attention to laws of the forum in which they are operating, since a one-size smart contract designed to fit all jurisdictions is not likely to be contractually binding.

Lastly, agreements entered with consumers through smart contracts should comply with the applicable consumer protection laws. Thus, in the EU, market participants are obliged to clearly define the material terms and conditions of the underlying transactions and make them available to their consumers. Particularly, EU consumers should be informed of the automatic and non-reversible nature of transactions executed through smart contracts.

Open Source Software

The collaborative nature of blockchain highly relies on open source software that frequently serves as a cornerstone to other innovations.

This model functions mostly because those who modify the open source software in the first place permit others to use their revised versions under the condition that they also allow the following versions to fall into the public domain. This scheme, broadly known as “copyleft,” may not, however, be necessarily recommended for permissioned blockchains. As discussed above, a U.S. or EU consortium is likely to allocate the ownership rights among the blockchain participants and might be hesitant to permit non-participants to use or modify their solutions. If that approach is the objective, such a consortium should carefully scrutinize the open source software used while developing a permissioned blockchain. Indeed, even unauthorized or inadvertent use of open source software distributed under a GNU-type license may force consortia to disclose and to share with others the technologies that constructed permissioned blockchains. On the other hand, a consortium that is considering incorporating open source software into its blockchain platform may want to use software that is distributed under MIT, BSD, or similar licenses, which permit less restrictive use.

Privacy

Although the United States does not have a single federal regulation that wholly addresses privacy, numerous public figures, including Apple CEO Tim Cook, have recently called for such a comprehensive law, sparking conversations and potential legislative action by the House of Representatives.

On the other hand, individual states, including California and Washington, have already passed, or are about to pass, GDPR-inspired regulations. For instance, California, in June 2018, created one of the strictest regulations for data collection and privacy practices of companies that conduct business in California. Although it does not go into effect until January, the California Consumer Privacy Act (CCPA) is likely to substantially impact blockchain platforms by potentially restricting the ability to transact or process broadly defined “personal information.” Indeed, the CCPA has duplicated the GDPR-inspired rights to access or deletion, among other rights. In addition, market participants in healthcare and financial industries should also keep in mind the existing federal laws, including the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA), that grant patients or financial services consumers far-reaching rights with respect to their personal information, rights which may directly conflict with the immobility of blockchains.

From the EU perspective, the GDPR and “privacy by design” have already influenced the architecture of blockchain solutions that “process” EU personal data. In instances wherein personal data is processed through blockchains, questions arise when qualifying market participants as either the data controllers or the data processors, which, consequently, determines the scope of legal obligations and financial liabilities for the participants. Due to blockchain’s decentralized architecture and the B2B cooperative approach, making such a determination may not be as simple as it sounds. Another key issue relates to blocks’ immutability—a fundamental blockchain feature—which may conflict with the individuals’ rights to rectification or erasure of their personal data. It is worth noting that the EU-level regulatory bodies, as well as particular member countries, are working on a sensible approach to address this issue.

Consortia that operate their platforms in the applicable jurisdictions, or process data of the residents of such jurisdictions, would be required to design and develop their platforms while “incorporating appropriate technical and organizational measures,” as required by Art. 25 of the GDPR, to ensure a level of security appropriate to the risk, among other privacy-related requirements.

Conclusion

Although faced with multiple challenges, many analysts believe the value of blockchain consortia may not be overstated. It is reasonable to assume that companies will continue to turn their attention and dedicate resources to blockchain consortia as a means of expanding their global reach. Following this expansion, legal counsel should closely follow the developments on both sides of the Atlantic Ocean to timely identify and respond to the dynamically changing blockchain landscape.

Michael Baumert is an associate in Barnes & Thornburg’s Chicago office. As a member of the Intellectual Property Department and Corporate Department, Michael focuses on technology-driven transactions, sourcing, cloud computing, and data privacy and security. Szymon Ciach and Piotr Galka are associates with SSW Pragmatic Solutions.