What IP Practitioners Should Know About Blockchain

Preston Byrne (Moderator)
Partner, Byrne & Storm, P.C.

Joshua Krumholz
Partner, Holland & Knight LLP

Jennifer Connors
Partner, Holland & Knight LLP

THE INTERSECTION OF BLOCKCHAIN AND INTELLECTUAL PROPERTY

By: Joshua C. Krumholz, Partner, Holland & Knight

1. BLOCKCHAIN BASICS ARE NOT PROTECTABLE

1.1. ***Satoshi Nakamota (his/her true identity is unknown) released the first white paper on blockchain in 2008 entitled "Bitcoin: A Peer to Peer Electronic Cash System"*** [1]

1.2. ***Bitcoin itself was first offered to the open source community in 2009*** [2]

1.3. ***The information disclosed in those works is now dedicated to the public***

1.4. ***One cannot patent, for example, the broad concepts of a distributed ledger system or known cryptography techniques, both of which form the bedrock of blockchain***

1.5. ***But iterations and applications of that foundational technology are very much in play***

2. MANY APPLICATIONS FOR BLOCKCHAIN EXIST

2.1. ***While the use of blockchain is still in its infancy, its potential application is considerable***

2.2. ***Examples of blockchain applications presently being used include:***

2.2.1. **HSBC.** HSBC recently announced that, through its new blockchain platform, it has reduced the costs for its foreign exchange trades by one quarter.[3]

2.2.2. **JPM Coin.** JP Morgan has announced that it is the first US bank to successfully test its first cryptocurrency coin, the JPM Coin.[4]

2.2.3. **The Boomerang Project**. The Boomerang Project is a blockchain-based platform that enables a global system of online reviews, loyalty rewards programs and tipping based on verified transactions with a focus on the "gig economy" that connects contracted service providers ('workers') with consumers via an online/mobile app platform. Since the platform will be

---

[1] https://www.forbes.com/sites/bernardmarr/2018/02/16/a-very-brief-history-of-blockchain-technology-everyone-should-read/#34fbf9067bc4

[2] https://www.forbes.com/sites/bernardmarr/2018/02/16/a-very-brief-history-of-blockchain-technology-everyone-should-read/#34fbf9067bc4

[3] https://www.reuters.com/article/us-hsbc-blockchain/hsbc-forex-trading-costs-cut-sharply-by-blockchain-executive-idUSKCN1Q31MW?utm_source=applenews

[4] https://www.jpmorgan.com/global/news/digital-coin-payments

decentralized and will not be owned by any single entity, it is expected to eliminate or reduce the number of unverified reviews and restore trust in ratings.

2.2.4. **Tari Tickets**. Event ticketing normalizes a market where artists, teams, promoters and venues do not share in any of the ticket resale revenue, which is a large and growing market. Currently, ticketing platforms underinvest in innovation and do not prioritize improving the user experience for all stakeholders. Tari Tickets uses a blockchain platform to provide ticketing and marketing services to the global live events industry.

2.2.5. **The Codex Project.** Without a central title registry for arts and collectibles items, it is difficult to verify ownership and trace ownership history when establishing a collectible item's value. Forgeries cost the arts and collectibles industry $6 billion a year in losses. Right now, there are currently several methods of sale in the art and collectibles market, including private sales, live actions, and timed auctions. All of these methods lack a centralized title registry for each asset class (fine art, wine, jewelry, watches, collectible cars, etc.). Tracking, identifying, and confirming that an item is legitimate has been a challenge—yet that's critical to valuation. To address those issues, Codex has developed The Codex Protocol, which is a registry built on the blockchain that can show ownership, transmission history, and metadata like past appraisals, restoration records, or photographs. The Codex Protocol provides a way for everyone to verify ownership while keeping it decentralized and anonymous. The protocol maintains accurate title records, enables arts and collectible transactions, streamlines auction operations, all while maintaining privacy of participants.

2.3. ***But there are hundreds more, and each involves technical development that may or may not be the proper subject of IP protection***

3. EXAMPLES OF ALLOWED PATENTS

3.1. ***In total, the Patent Office has allowed over 260 patents related to blockchain***

3.2. ***Applications have risen steadily:***

3.2.1. In 2016, patent filings totaled 521[5]

3.2.2. In 2017, that number rose to 602[6]

3.2.3. Although it is hard to get precise numbers, in total, the number of applications has risen to over 1500

3.3. ***Chinese entities have constituted the largest number of filers, accounting for 56% of all applicants in 2017***[7]

3.4. ***Examples of subject-matter that has been allowed by the Patent Office includes:***

3.4.1. U.S. Patent No. 10,055,446 (Ensuring data integrity of executed transactions)

[5] https://blogs.thomsonreuters.com/answerson/in-rush-for-blockchain-patents-china-pulls-ahead
[6] https://blogs.thomsonreuters.com/answerson/in-rush-for-blockchain-patents-china-pulls-ahead
[7] https://blogs.thomsonreuters.com/answerson/in-rush-for-blockchain-patents-china-pulls-ahead

3.4.1.1. The patent claims a central service provider that receives transaction data describing a first set of transactions, and receives transaction data from a primary recordation system describing a second set of transactions recorded by the primary recordation system. The primary recordation system can request and subsequently verify executed transactions and party positions with the central service provider that maintains the blockchain records. This permits the primary recordation system to maintain its role in servicing requests from various parties while the blockchain system of the central service provider provides additional transaction verification and confirmation. The elements of the claims directly involve an improvement in the field, specifically providing that the data state of the blockchain maintained by the central service provider can serve as a backup to a primary recordation system. As such, if a discrepancy arises (e.g. due to a missed, extra, or wrongful execution of a transaction or unauthorized change), the discrepancy can be readily identified and traced

3.4.2. U.S. Patent No. 9,875,510 (Consensus system for tracking peer-to-peer digital records)

3.4.2.1. The patent claims that it directly improves existing technological processes in digital object tracking and management. The disclosure describes a peer-to-peer consensus system and method for achieving consensus in tracking transferrable digital objects and preventing double spending by using a “most committed stake metric” to choose a single consensus transaction record. The most committed stake metric allows for a more complete and preserved history of block production and does not require block signers to sign a block unless the block references every prior block they’ve signed. Further, the most committed stake metric eliminates abandoned fork chains/blocks that are otherwise absent from the consensus chain, and facilitates detection and prevention in a fork resolution, which ultimately occurs via majority vote of stake. Further, participants can vote for fork chains automatically via transactions (which include a hash of a recent block from the consensus chain as known to the creator of the transaction). When there is a fork, the transactions will reference a recent block on the widest fork chain, and are only valid on the fork chain that they reference. Thus, these transactions add to the width of the already widest fork chain and resolve the fork to a single consensus chain

3.4.3. U.S. Patent No. 9,807,106 (Mitigating blockchain attack)

3.4.3.1. The patent claims a mechanism for detecting and mitigating threats to blockchain environments. It requires defining a transaction creation profile, submitting a transaction to the blockchain, which in turn causes the generation of a profiler data structure in the blockchain to generate profile transactions to be submitted to the blockchain according to the transaction creation profile, monitoring the blockchain to identify profile transactions and then comparing identified profile transactions with the transaction creation profile to detect a deviation from the transaction creation profile

4. THE ROLE AND IMPACT OF OPEN SOURCE SOFTWARE

4.1. ***Blockchain networks are typically built upon open source software, which can have a substantial impact on a developer's IP rights***

4.2. ***Open source software versus proprietary software***

4.2.1. The term "open source software" refers to software that is distributed in source code form. In source code form, the software can be tested, modified, and improved by people other than the developer who created the code in the first place

4.2.2. The term "proprietary" software refers to software that is distributed in object code form only. With proprietary software, the developer does not distribute the source code, but rather protects it as a trade secret. As a result, others are unable to modify, maintain, or have visibility into its software code base

4.3. ***Blockchain networks generally***

4.3.1. Public platforms

4.3.1.1. In a public network, each node of the network contains all transactions, the nodes are anonymous, and the participants are unknown to each other

4.3.1.2. Bitcoin and Ethereum are the leading public blockchain platforms[8]

4.3.2. Permissioned platforms

4.3.2.1. In a permissioned network, network members are vetted, unacceptable members are excluded, the nodes are not anonymous, and transactional information can be selectively disclosed to some, and not all, nodes

4.3.2.2. Hyperledger, Corda, and Enterprise Ethereum are the "big three" leading commercial, permissioned blockchain platforms[9]

4.4. ***The role of open source software licenses with blockchain platforms***

4.4.1. The software code bases for Bitcoin,[10] public Ethereum,[11] and Hyperledger,[12] and portions of the software code bases for Enterprise Ethereum[13] and Corda,[14] all consist of open source software

---

[8] R. Brown, "Corda: Open Source Community Update" (May 13, 2018) located at https://medium.com/corda/corda-open-source-community-update-f332386b4038.
[9] R. Brown, "Corda: Open Source Community Update" (May 13, 2018) located at https://medium.com/corda/corda-open-source-community-update-f332386b4038.
[10] *See* http://www.Bitcoin.org.
[11] L. Zeug, "Licensing" (September 4, 2016), located at https://github.com/ethereum/wiki/wiki/Licensing.
[12] "About Hyperledger," located at https://www.hyperledger.org/about.
[13] Enterprise Ethereum Alliance Specification Clears the Path to a Global Blockchain Ecosystem (May 16, 2018), located at https://entethalliance.org/enterprise-ethereum-alliance-specification-clears-path-global-blockchain-ecosystem/.

4.4.2. To use open source software, one must comply with the licensing requirements associated with that software, which will vary from one open source software to another. Each of the licenses, however, can have a substantial impact on a user's intellectual property rights

4.4.3. Generally, open source software licenses range from:

4.4.3.1. Permissive licenses, which allow licensees royalty-free and essentially unfettered rights to use, modify, and distribute applicable software and source code,[15] to

4.4.3.2. Restrictive, "copyleft" licenses, that place significant conditions on modification and distribution of the applicable software and source code

4.4.4. Two open source licenses are of particular import with regard to blockchain networks:

4.4.4.1. The General Public License, Version 3,[16] which governs large portions of the Ethereum code base,[17] and

4.4.4.2. The Apache 2.0 license[18] which governs open source software provided via the Hyperledger, Corda, and Enterprise Ethereum platforms[19]

4.5. *General Public License, Version 3 ("GPLv3") (Ethereum)*

4.5.1. GPLv3 is known as a strong copyleft license

4.5.2. To the extent that a developer incorporates GPLv3 code into his/her proprietary code, that developer must make his/her proprietary source code publicly available and at no charge, and may not restrict the use of that source code through copyright laws or otherwise

---

[14] "Contributing to Corda," located at https://github.com/corda/corda/blob/master/CONTRIBUTING.md; Downloads: DemoBench for Corda 3.0, located at https://www.corda.net/downloads/.
[15] Bitcoin software, for example, is licensed under the permissive, MIT License. See http://www.Bitcoin.org; https://opensource.org/licenses/MIT.
[16] GPLv3 license, located at https://www.gnu.org/licenses/gpl-3.0.en.html .
[17] L. Zeug, "Licensing" (September 4, 2016), located at https://github.com/ethereum/wiki/wiki/Licensing. *See, e.g.*, Ethereum-sandbox License, located at https://github.com/ether-camp/ethereum-sandbox/blob/master/LICENSE.txt.
[18] Apache 2.0 license, located at https://www.apache.org/licenses/LICENSE-2.0.
[19] For Corda, *see* R. Brown, "Corda: Open Source Community Update" (May 13, 2018) located at https://medium.com/corda/corda-open-source-community-update-f332386b4038; "Contributing to Corda," located at https://github.com/corda/corda/blob/master/CONTRIBUTING.md. For Hyperledger, *see* Brian Behlendorf, "Meet Hyperledger: An 'Umbrella' for Open Source Blockchain & Smart Contract Technologies" (September 13, 2016) located at https://www.hyperledger.org/blog/2016/09/13/meet-hyperledger-an-umbrella-for-open-source-blockchain-smart-contract-technologies. Code contributed to the Enterprise Ethereum Alliance is generally made available under an open source license that mirrors the Apache 2.0 license, *see* Enterprise Ethereum Alliance Inc. Intellectual Property Rights Policy, available at https://entethalliance.org/join/.

4.5.3. Further, to the extent that the developer possesses patents that cover his/her proprietary code, the developer also must provide others with a royalty-free license to use the patents to the extent necessary to use the code

4.5.4. Finally, by using GPLv3 code, the developer cannot sue others for patent infringement to the extent they are using the GPLv3 code

4.5.5. In short, if a developer uses GPLv3 code, any code that he/she created that is based on the GPLv3 code becomes part of the public domain and free for anyone to use

4.6. ***Apache 2.0 license ("Apache") (Hyperledger, Corda and Enterprise Ethereum)***

4.6.1. Apache is more flexible than GPLv3

4.6.2. The impact can be similar to GPLv3 with respect to one's IP rights, but only if the developer affirmatively contributes its software to the maintainer of the Apache code at issue; in other words, it is not enough to simply use the open source software, the developer must affirmatively contribute whatever proprietary software he/she has created

4.6.3. In other words, the developer is free to use Apache code in his/her own proprietary code without a limitation of IP rights

4.6.4. In addition, a developer can still sue another Apache user for patent infringement; if he/she does, however, the developer's right to use the Apache code terminates

4.7. ***Based on the foregoing, one would assume that companies would stay away from restrictive usage, but that has not always been the case***

4.7.1. IBM, for example, has contributed code under the Apache license to the Hyperledger platform, and in turn is providing commercial Blockchain-as-a-Service (BaaS) offerings based on this platform using IBM's cloud infrastructure[20]

4.7.2. Microsoft has similar commercial offerings, based on Azure and the Enterprise Ethereum platform[21]

4.8. ***Making conscious choices***

4.8.1. The bottom line, however, is that the network that a company chooses can have an impact on that company's IP rights

4.8.2. Choosing a network is a technical one, typically made by IT professionals within the company

[20] IBM Blockchain, The Founder's Handbook: Your guide to getting started with Blockchain (Edition 2.0) located at https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=28014128USEN.
[21] M. Finley, Getting Started with Ethereum using Azure Blockchain (January 24, 2018), located at https://blogs.msdn.microsoft.com/premier_developer/2018/01/24/getting-started-with-ethereum-using-azure-blockchain/

4.8.3. It is important for a company's legal department to be involved in that decision before significant investments are made in developing a blockchain product

5. THE THREAT OF (NON-PATENT) LITIGATION

5.1. ***Blockchain has the potential of being a highly disruptive technology***

5.1.1. Its potential applications include:

5.1.1.1. Financial transactions

5.1.1.2. Supply chain management

5.1.1.3. Real estate transactions and ownership

5.1.1.4. IP transactions and ownership

5.1.1.5. Health care

5.1.1.6. And many others

5.1.2. Most disruptive technologies generate litigation

5.2. ***Fraud cases***

5.2.1. Fraud cases have been by far the most prevalent so far. The vast majority, if not all, blockchain litigation has focused on cryptocurrency issues, and in particular where fraud has been committed in connection with specific cryptocurrency transactions.[22]

5.2.2. In addition to private lawsuits, five different federal regulators have brought suit, and state regulators have brought 46 separate administrative actions in thirteen states.[23]

5.3. ***Litigation by threatened stakeholders***

5.3.1. Disruptive technologies can make many enemies, namely the stakeholders that were once well-positioned but become displaced by the new technology.

5.3.2. Here the most obvious are third-party intermediaries that presently are necessary to mediate complex financial transactions, particularly trans-border transactions.

5.3.3. Another example involves logistics providers that mediate the complexities associated with supply chain management.

5.3.4. As changes are implemented, any blockchain adopter needs to consider the rights of these third parties, including their intellectual property rights, and make sure that those rights are addressed before litigation ensues.

5.4. ***Litigation by blockchain partners***

[22] www.blockchaincenter.com
[23] *Id.*

5.4.1. Because setting up a blockchain network is a complicated process, often involving many partners, disputes can arise between those partners and each other's rights.

5.4.2. Issues that should be preemptively considered include:

5.4.2.1. Understanding what intellectual property rights have been created through the construction of the blockchain network.

5.4.2.2. Establishing which rights belong to whom.

5.4.2.3. Understanding, per above, the impact that open source usage has on those rights.

5.4.2.4. Assessing what information can and cannot be shared by the members of the network.

5.4.2.5. Agreeing upon respective rights to administer, maintain, modify and operate the network, and credential new members.

6. THE THREAT OF PATENT LITIGATION

6.1. ***The largest threat, however, is the threat that has not yet arrived: the threat of patent litigation***

6.2. ***The present state of patent litigation***

6.2.1. After a number of years of heavy patent litigation, the size and amount of patent litigation matters has decreased in recent years

6.2.2. That reduction has been the result of many factors, but the key contributors are:

6.2.2.1. The creation of *inter partes review* proceedings, which have given defendants an opportunity to invalidate patents through the patent office, often staying proceedings in federal court during that process

6.2.2.2. Stricter requirements on proving damages, and the reversal by the Federal Circuit of many large district court awards

6.2.2.3. New defenses—in particular so-called *Alice* defenses—that may be interjected at the beginning of a case and that can result in an early dismissal

6.2.2.4. Patent pools and other organizations that acquire patents before they are acquired by patent trolls, and license those patents to their membership

6.2.2.5. Many of the most powerful patents in a broad range of industries already have been licensed

6.3. ***Blockchain may usher in a new wave of patent litigation***

6.3.1. History tells us that, notwithstanding the changes in the law discussed above and the constraints imposed by open source licenses, blockchain is likely to usher in a new wave of patent litigation

6.3.2. The reasons for that include:

6.3.2.1. Blockchain is creating a new set of patents, based on new technology, that have not been licensed

6.3.2.2. Blockchain technology likely will be used as fundamental building blocks, making the technology more valuable and damages more lucrative

6.3.2.3. Blockchain technology will be used in lucrative fields which, by association, will make blockchain patents more valuable

6.3.2.4. In a competitive landscape, certain companies will try to use their patents to keep competitors out of the marketplace

6.3.3. Patent trolls see the opportunity

6.3.3.1. A real indicator of the opportunity is the presence of patent troll investment in a field, which is the case with blockchain

6.3.3.2. Eric Spangenburg, a well-known founder of non-practicing entities ("NPEs"), has set up IPWE to collect and exploit blockchain patents, and Intellectual Ventures, a well-known and well-financed NPE, similarly is seeking to acquire and exploit patents in this area

6.4. ***Reasons to acquire patents in the field***

6.4.1. Offensive use

6.4.1.1. Blockchain technology is starting to become a crowded field. Some companies' entire business models are based on the creation of blockchain technologies. For those companies, acquiring and asserting patents may be the only way for them to effectively compete

6.4.1.2. Other companies may see an opportunity to monetize their R&D efforts through the licensing of their blockchain patent portfolio

6.4.2. Defensive use

6.4.2.1. As blockchain matures, patent leaders will emerge, and to avoid mutual destruction, they will enter into cross-licenses with each other

6.4.2.2. Other companies, in contrast, will try to enter the industry without a proper patent portfolio, and may find significant barriers to entry if the patent leaders seek to assert their right to exclude those other companies from using their patented technology

6.4.2.3. So the bottom line is that any major player in the blockchain field needs patents to at least cross-license with its major competitors

6.4.2.4. And acquiring patents can also stop another company from patenting the same idea and asserting it against you

6.5. ***Strategies for limiting patent litigation exposure include:***

6.5.1. **Join patent pools.** Patent pools are membership-based organizations that acquire patents, or take licenses on patents, for the benefit of their members

6.5.2. **Actively enter into cross-license agreements.** If a company has an existing portfolio, consider approaching other major players in the blockchain field to enter into cross-licenses with those companies

6.5.3. **Monitor patent application and allowed patents.** Review patent applications as they are published (18 months after filing) and when patents issue to take preventative action on those patents

6.5.4. **Consider design-arounds where available.** To the extent a company identifies potentially problematic patents or applications, an option for it is to "design around" the problematic patent

6.5.5. **Be prepared to file IPRs.** To the extent a company finds a problematic patent, one option is to file an IPR with the Patent Office to try to invalidate the patent

6.5.6. **Prepare open source defenses.** At a minimum, investigate whether the lawsuit violates an open source license agreement

6.5.7. **Attack the patents on *Alice* grounds.** If a company ends up in litigation, it still may be able to terminate that litigation early by filing an *Alice* motion because the concept of blockchain itself is an abstract idea, and not patentable as such

6.5.8. **Assert counterclaims.** As discussed above, it is important for a company to acquire its own patent portfolio. If successful in doing so, and if sued by a practicing company, that company may be able to assert its own claims of patent infringement. Doing so typically makes it easier to resolve a dispute in its early stages

7. THE ROLE OF BLOCKCHAIN STANDARDS

7.1. ***Industry standards***

7.1.1. Industry standards refer to technical specifications that industry members agree to use in their products.

7.1.2. Industry standards are collaboratively developed through Standards Setting Organizations (or "SSO"). Periodically, the SSO will hold meetings where industry players will propose and debate differing proposals regarding how a technology should operate

7.1.3. Decisions regarding proposals, and the final technical specifications that stem from them, are reached by consensus by the participants

7.2. ***Blockchain standards are presently being created:***

- The International Standards Organization ("ISO") has formed Technical Committee 307 ("ISO/TC 307") to consider blockchain and distributed ledger technologies.[24]

- The Institute of Electrical and Electronics Engineers ("IEEE") has formed two blockchain groups: (1) Project 2418 to develop a standard framework for the use of blockchain in Internet-of-Things applications;[25] and (2) Project 825 to develop a guide for interoperability of blockchains for energy transaction applications.[26]

- The Blockchain in Transportation Alliance ("BiTA") is focused on the use of blockchain in freight payments, asset history, chain of custody, smart contracts and other related goals.[27]

- The Enterprise Ethereum Alliance recently released an architecture stack designed to provide the basis for an open-source, standards-based specification to advance the adoption of Ethereum solutions for commercial, permissioned networks (referred to as "Enterprise Ethereum").[28]

7.3. ***Lessons from the wireless industry***

7.3.1. Standards have had a dramatic effect, both positive and negative, on the wireless industry

7.3.2. Industry standards have essentially allowed the wireless industry to blossom by:

7.3.2.1. Ensuring compatibility between and among devices and equipment

7.3.2.2. Creating a framework that optimizes the best technologies

7.3.2.3. Creating a safe framework for investment and adoption

7.3.2.4. Allowing for better planning with more accurate forecasts

7.3.3. There are disadvantages to standards as well:

7.3.3.1. To a degree, they can level out the playing field

7.3.3.2. Alternative standards often compete with each other before adoption, and companies can invest in the wrong standard

[24] https://www.iso.org/committee/6266604.html.
[25] http://standards.ieee.org/develop/project/2418.html.
[26] http://standards.ieee.org/develop/project/825.html.
[27] https://bita.studio.
[28] Enterprise Ethereum Alliance Advances Web 3.0 Era with Public Release of the Enterprise Ethereum Architecture Stack (May 2, 2018), located at https://entethalliance.org/enterprise-ethereum-alliance-advances-web-3-0-era-public-release-enterprise-ethereum-architecture-stack/; https://entethalliance.org/wp-content/uploads/2018/05/EEA-TS-0001-0-v1.00-EEA-Enterprise-Ethereum-Specification-R1.pdf.

7.3.3.3. Companies are held captive to certain required features and functions, and may need to use others' patents to enable those features and functions

7.3.3.4. SSOs are less nimble than individual companies to make technical changes

7.3.4. There are good reasons for the blockchain industry to invest in the creation of industry standards. Blockchain is based on networks that are large enough—*i.e.* have enough nodes—to create reliability. As such, interoperability and scalability are important. Standardization of blockchain elements can be an important tool in achieving those goals

7.3.5. The standardization process often involves competing visions. Certain companies will advance one approach, and other companies will advance a different approach. That advocacy typically is based on a good faith belief, but it also arises from investments that companies make in their technology

7.3.6. A meaningful standardization process contains both risk and opportunity because no company wants to be make the wrong bet and become the Betamax of blockchain technology. Companies therefore need to be thinking hard about the competing standards that are being created and what role they wish to play in that creation. An entirely passive role can result in other thought leaders seizing the marketplace, but too aggressive a role can lead to massive investments that are not adopted by the marketplace as a whole

7.4. ***The impact of industry standards on blockchain IP***

7.4.1. From an IP perspective, the creation of standards can have a significant impact

7.4.2. If a company's patented technology is adopted into a standard, it becomes a "standards-essential" patent, meaning that everyone in the industry must practice it to comply with the standard

7.4.3. In that situation, the company holding the patent is compelled to license the patent to others under FRAND (fair, reasonable and non-discriminatory) terms, which of course can be a matter of much debate

7.4.4. And many patent trolls will claim that their patents are essential to compliance with a standard, which can change the complexion of a litigation

Blockchain & Cryptocurrency Regulation

2019

First Edition

Contributing Editor
Josias Dewey

CONTENTS

Preface	Josias Dewey, *Holland & Knight LLP*	
Foreword	Aaron Wright, *Enterprise Ethereum Alliance*	
Glossary	The Editor shares key concepts and definitions of blockchain	
Industry	*Promoting innovation through education: The blockchain industry, law enforcement and regulators work towards a common goal* Jason Weinstein, Alan Cohn & Chelsea Parker, *The Blockchain Alliance*	1
	The loan market, blockchain, and smart contracts: The potential for transformative change Bridget Marsh, *LSTA*, & Josias Dewey, *Holland & Knight LLP*	5
	An overview of the Wall Street Blockchain Alliance Ron Quaranta, *Wall Street Blockchain Alliance*	14
General chapters	*Blockchain and Intellectual Property: A case study* Joshua Krumholz, Ieuan G. Mahony & Brian J. Colandreo, *Holland & Knight LLP*	18
	Initial Coin Offerings: A comparative overview of securities regulatory environments in the US, UK and Asia Pacific Justin Cooke, Richard Cohen & Jason Denisenko, *Allen & Overy LLP*	34
	The custody of digital assets Jay G. Baris, *Shearman & Sterling LLP*	47
	Mutually assured disruption: The rise of the security token Joshua Ashley Klayman, *Klayman LLC & Inflection Point Blockchain Advisors, LLC*	60
	Cryptocurrency and other digital assets for asset managers Gregory S. Rowland & Trevor I. Kiviat, *Davis Polk & Wardwell LLP*	90
	The yellow brick road for consumer tokens: The path to SEC and CFTC compliance David L. Concannon, Yvette D. Valdez & Stephen P. Wink, *Latham & Watkins LLP*	101
	Custody and transfer of digital assets: Key U.S. legal considerations Michael H. Krimminger, Colin Lloyd & Sandra Rocks *Cleary Gottlieb Steen & Hamilton LLP*	121
	An introduction to virtual currency money transmission regulation Michelle Ann Gitlitz & Grant E. Buerstetta, *Blank Rome LLP*	132
	The rise of the crypto asset investment fund: An overview of the crypto fund ecosystem Jonathan Cardenas, *Yale Law School*	149
	Cryptocurrency compliance and risks: A European KYC/AML perspective Fedor Poskriakov, Maria Chiriaeva & Christophe Cavin, *Lenz & Staehelin*	163
	Aspects of state securities regulation Greg Strong & Rodrigo Seira, *DLx Law, LLP*	175
	The regulation of blockchain technology Joseph F. Borg & Tessa Schembri, *WH Partners*	188

Country chapters

Argentina	Juan M. Diehl Moreno & Santiago E. Eraso Lomaquiz, *Marval, O'Farrell & Mairal*	193
Australia	Peter Reeves & Georgina Willcock, *Gilbert + Tobin*	198
Austria	Ursula Rath & Thomas Kulnigg, *Schönherr Rechtsanwälte GmbH*	209
Belgium	Muriel Baudoncq & France Wilmet, *Janson Baugniet*	216
Bermuda	Michael Hanson & Adam Bathgate, *Carey Olsen Bermuda*	226
British Virgin Islands	Clinton Hempel & Mark Harbison, *Carey Olsen*	237
Canada	Conrad Druzeta, Simon Grant & Matthew Peters, *Bennett Jones LLP*	243
Cayman Islands	Alistair Russell & Dylan Wiltermuth, *Carey Olsen*	254
China	Lefan Gong & Luping Yu, *Zhong Lun Law Firm*	262
Cyprus	Karolina Argyridou, *K. Argyridou & Associates LLC*	268
Estonia	Priit Lätt & Carel Kivimaa, *PwC Legal*	273
France	Christophe Perchet, Juliette Loget & Stéphane Daniel, *Davis Polk & Wardwell LLP*	283
Germany	Dennis Kunschke & Dr. Stefan Henkelmann, *Allen & Overy LLP*	292
Gibraltar	Joey Garcia & Jonathan Garcia, *ISOLAS LLP*	305
Guernsey	David Crosland & Felicity White, *Carey Olsen LLP*	314
Hong Kong	Yu Pui Hang, *L&Y Law Office / Henry Yu & Associates*	325
India	Ashwin Ramanathan, Anu Tiwari & Rachana Rautray, *AZB & Partners*	335
Ireland	Maura McLaughlin, Pearse Ryan & Caroline Devlin, *Arthur Cox*	342
Japan	Taro Awataguchi, *Anderson Mōri & Tomotsune*	349
Jersey	Christopher Griffin, *Carey Olsen*	359
Korea	Jung Min Lee, Samuel Yim & Joon Young Kim, *Kim & Chang*	367
Liechtenstein	Dr. Ralph Wanger & Laura Johann, *BATLINER WANGER BATLINER Attorneys at Law Ltd.*	373
Malta	Malcolm Falzon & Alexia Valenzia, *Camilleri Preziosi Advocates*	378
Mexico	Juan Carlos Tejado & Miguel Gallardo Guerra, *Bello, Gallardo, Bonequi y Garcia, S.C.*	386
Netherlands	Björn Schep, Christian Godlieb & Willem Röell, *De Brauw Blackstone Westbroek*	395
Portugal	Filipe Lowndes Marques, Mariana Solá de Albuquerque & João Lima da Silva, *Morais Leitão, Galvão Teles, Soares da Silva & Associados, Sociedade de Advogados, SP, RL*	403
Russia	Vasilisa Strizh, Dmitry Dmitriev & Anastasia Kiseleva, *Morgan, Lewis & Bockius LLP*	412
Singapore	Franca Ciambella, En-Lai Chong & YingXin Lin, *Consilium Law Corporation*	420
South Africa	Angela Itzikowitz, Ina Meiring & Era Gunning, *ENSafrica*	432
Spain	Alfonso López-Ibor, Pablo Stöger & Zhongbo Jin, *Ventura Garcés & López-Ibor Abogados*	438
Switzerland	Daniel Haeberli, Stefan Oesterhelt & Urs Meier, *Homburger*	443
Taiwan	Robin Chang & Eddie Hsiung, *Lee and Li, Attorneys-at-Law*	454
UAE	Joby Beretta, *The Bench*	459
United Kingdom	Simon Lovegrove & Albert Weatherill, *Norton Rose Fulbright LLP*	469
USA	Josias Dewey, *Holland & Knight LLP*	479
Venezuela	Luisa Lepervanche, *Mendoza, Palacios, Acedo, Borjas, Páez Pumar & Cía. (Menpa)*	488

Blockchain and intellectual property: A case study

Joshua Krumholz, Ieuan G. Mahony & Brian J. Colandreo
Holland & Knight LLP

Introduction

As discussed elsewhere in this book, blockchain has the potential for transformational change. Like most transformational technologies, its development and adoption are laden with intellectual property ("IP") issues, concerns and strategies. Further, given the potentially wide-ranging impact of blockchain technology, the public and private nature of its application, and the prevalent use of open source software, blockchain raises particularly unique IP issues.

The purpose of this chapter is to help the practitioner identify some of the issues that may affect blockchain development and adoption. We address these issues as they may relate to a company's creation of its own IP, and as they may relate to efforts by others to assert their IP against a company. We discuss the issues in the context of the hypothetical scenario discussed below.

The hypothetical transaction

Although many sectors stand to benefit from the use of blockchain technology, the financial and supply chain management sectors may be among the first to benefit. For purposes of discussion, this chapter focuses on the financial sector, and in particular the following hypothetical:

> *A U.S. company is building a new platform using distributed ledger technology for its syndicated loan transactions. Many participants are involved in a typical transaction serviced by the platform, including borrowers, lenders, an administrative agent, credit enhancers and holders of subordinated debt. The platform that the company is building employs smart contracts to effectuate the functionality over a permissioned (private) network with several hundred nodes in the network.*

Our hypothetical company, as noted, has chosen to deploy its solution via a permissioned network. A blockchain developer has two broad options in this regard. First, the developer could select a public blockchain network for its platform. In a public network, each node contains all transactions, the nodes are anonymous, and participants are unknown to each other. Second, the developer could select a permissioned network (as our hypothetical company has). In a permissioned network, the network owner vets network members, accepts only those that it trusts, and uses an access control layer to prevent others from accessing the network. Unlike the nodes on a public network, the nodes on a permissioned

network are not anonymous. In addition, a permissioned network can be structured so that specified transactions and data reside only on identified nodes, and are not stored on all nodes in the network.[1] In certain commercial transactions, participants must be known to each other in order to meet regulatory requirements, such as those designed to prevent money laundering. In these situations, a network of anonymous nodes would not be compliant.

Our hypothetical company has selected a permissioned network, we can assume, to obtain these benefits. This selection comes with costs, however, and the company will lose the benefit, for example, of validating a transaction over the full multitude of distributed nodes in a public blockchain network, and the assurances of immutability that that provides.

The blockchain patent landscape

Since Satoshi Nakamoto published the Bitcoin whitepaper in 2008,[2,3] the number of blockchain patent applications has steadily risen. In 2016, applicants filed 521 patents related to blockchain technologies in the United States.[4] In 2017, the number of filings rose to 602.[5] Notably, Chinese entities filed the greatest number of U.S. blockchain patent applications in 2017, accounting for 56% of all filed applications.[6] Applications for blockchain patents filed by U.S. entities accounted for 22% during that same period.[7]

The United States Patent and Trademark Office has begun to issue blockchain patents based on these filings. Below is a breakdown of the largest holders of blockchain patents as of early 2018.[8]

Entity	Industry	No. of blockchain patents
Bank of America	Finance	43
MasterCard	Finance	27
IBM	Technology	27
Fidelity	Finance	14
Coinbase	Finance	13
World Award Foundation / World Award Academy / AMobilePay, Inc.	IP holding	12
TD Bank	Finance	11
402 Technologies S.A.	IP holding	10
Accenture	Technology	9
Dell	Technology	8

Because blockchain technology assists in the efficient and secure transfer of assets, it is no surprise that the financial industry currently dominates the blockchain patent space. Technology companies like IBM[9] and Dell[10] also are utilising blockchains to improve existing technologies and processes, including supply chain and digital rights management. The IP holding companies, meanwhile, presumably seek patents solely to monetise them.

What can be protected?

Only new and novel ideas may be patented

Ideas that already are in the public domain may not be patented, and much of blockchain technology falls into that category. As discussed elsewhere in this book, a blockchain is a distributed ledgering system that allows for the memorialising of transactions in a manner that is not easily counterfeited, is self-authenticating, and is inherently secure. The

basic concept of a blockchain may not be patented. A ledgering system that records such transactions, employs multiple identical copies of the ledgers, and maintains them in separate and distinct entities, similarly may not be patented as a new and novel idea. Blockchain technology also uses cryptography. Known cryptography techniques, even if used for the first time with blockchain, also are not likely to be patentable unless the combination resulted from unique insights or efforts to overcome unique technical problems.

Anyone is generally free to use these concepts and, as such, they are not patentable. So what is left that can be protected? Only novel and non-obvious ways to use the above-described blockchain distributed ledger system may be protected. For example, the traditional banking industry utilises central banks and clearing houses to effectuate the transfer of money between entities, which often results in significant delay to complete the transactions. With access to overnight shipping, real-time, chat-based customer service, and social networks allowing for the live-video conferencing of multiple parties positioned around the globe, it is understandable that today's consumer could be disillusioned with the pace at which financial transactions move through the traditional banking industry.

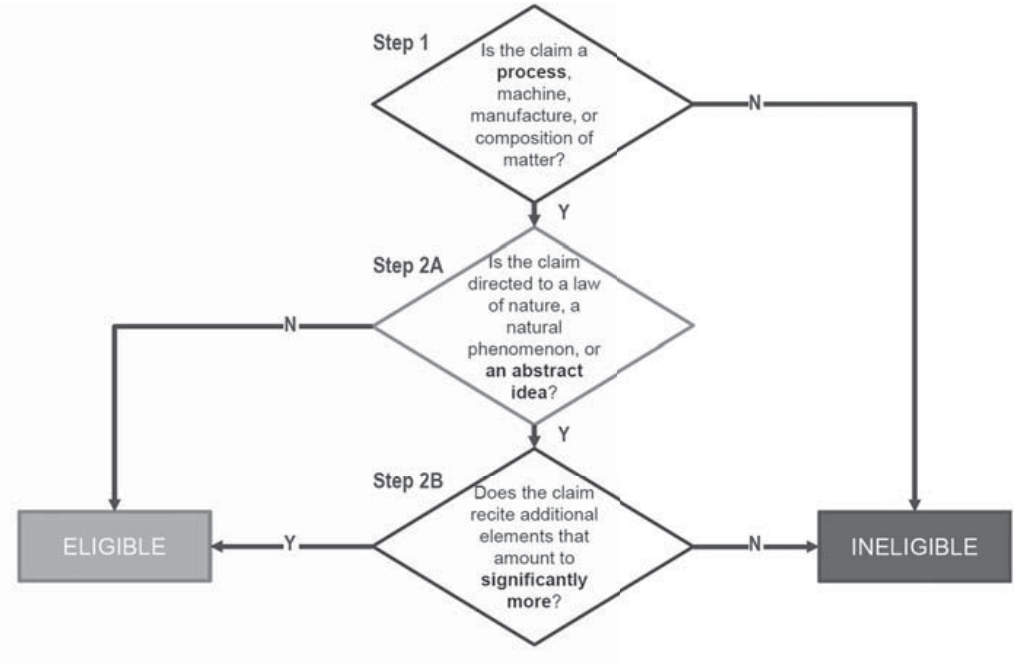
Accordingly, various companies and entities are devoting considerable time and resources to refining and revising the manner in which the traditional banking industry effectuates such monetary transactions. Entrepreneurial companies are inventing unique systems for effectuating asset transfers between banking entities that are memorialised via the above-described blockchain distributed ledgering system, as well as unique systems for expanding the utility of distributed ledgers via remote (and cryptographically-secured) content defined within the distributed ledgers. These improvements, as a general proposition, build and improve upon the foundational blockchain technology. Such an improvement could take the form, for example, of an application deployed on the "foundation" of the Hyperledger platform, and designed to verify the identity of participants in the hypothetical company's permissioned network, or to create audit trails for transactions on this network. It is these incremental improvements that potentially may be patentable. And it is in this area that our hypothetical company should be focusing its patenting efforts.

The *Alice* decision

Obtaining a patent by our hypothetical company also faces another obstacle. As explained by the Supreme Court in *Alice Corp. v. CLS Bank Int'l*, to be patentable, a claimed invention must be something more than just an abstract idea.[11] Rather, it must involve a technical solution to a specific problem or limitation in the field. In the *Alice* case, for example, a computer system was used as a third-party intermediary between parties to an exchange, wherein the intermediary created "shadow" credit and debit records (*i.e.*, account ledgers) that mirrored the balances in the parties' real-world accounts at "exchange institutions" (*e.g.*, banks). The intermediary updated the shadow records in real time as transactions were entered, thus allowing only those transactions for which the parties' updated shadow records indicated sufficient resources to satisfy their mutual obligations.

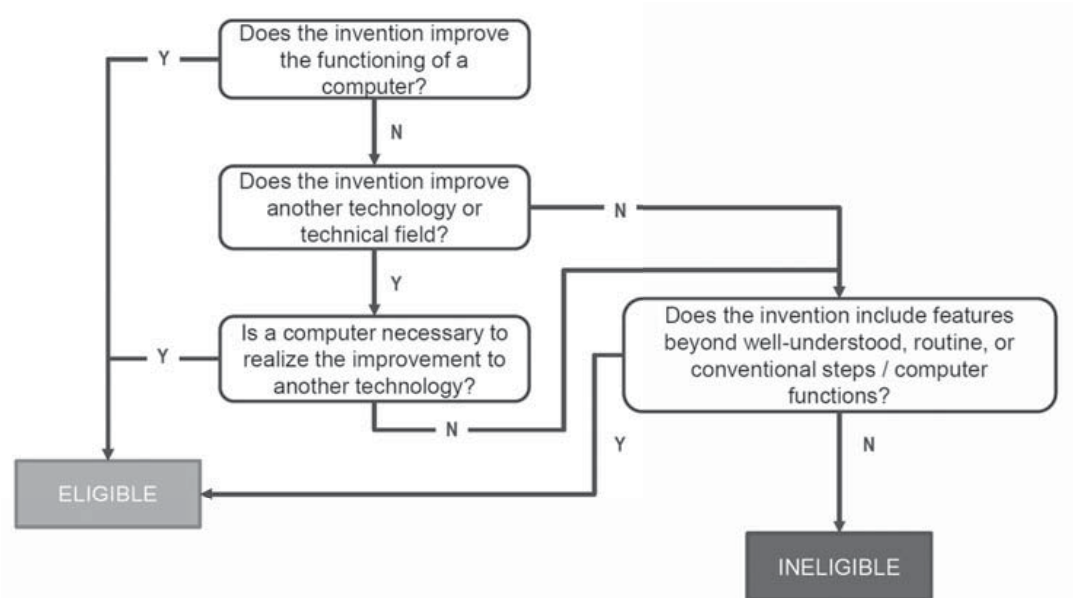
The Supreme Court held that, "[O]n their face, the claims before us are drawn to the concept of intermediated settlement, *i.e.*, the use of a third party to mitigate settlement risk." The Court went on to explain that "[T]he concept of intermediated settlement is a fundamental economic practice long prevalent in our system of commerce." The Court then explained that such basic economic principles could not be patented, even if implemented in software or in some other concrete manner, because abstract ideas are not themselves patentable. Allowing patents on abstract ideas themselves, the Supreme Court explained, would significantly restrict and dampen innovation.

The following flowchart defines the manner in which the patentability of subject matter should be analysed with respect to the *Alice* decision:



As such, basic concepts, even as they relate to blockchain, may not be patentable. So our hypothetical company must present more than just basic, economic principles in order to get a patent. It must, for example, claim specific improvements to the functioning of a computer, improvements to other, related technology, effect a transformation of a particular article to a different state or thing, add a specific implementation that is not well-understood, routine or conventional, or add unconventional steps that confine the claim to a particular useful application.

The following flowchart may be utilised when assessing the patentability of subject matter with respect to the *Alice* decision:



If the *Alice* decision taught practitioners anything, it is that IP law is continuously changing. Accordingly, just as a sound investment plan requires a diversified securities portfolio, a sound IP strategy requires a diversified IP portfolio. Therefore, companies should not put all of their proverbial eggs into one IP basket. For example, if a company was in the "intermediated settlement" space and all they owned were U.S. utility patents, the *Alice* decision would have been devastating to it.

Accordingly, companies should include utility patents in their IP portfolio. But the prudent company also would include design patents (for protecting, *e.g.*, user interfaces); trade secrets (for protecting, *e.g.*, backend algorithms that are not susceptible to reverse engineering); trademarks (for protecting the goodwill associated with the products produced by the company); service marks (for protecting the goodwill associated with the services provided by the company); copyrights (for protecting software code, and/or the expression of a concept or an idea); and various IP agreements (*e.g.*, employment agreements, development agreements, and licensing agreements). The best IP portfolio for our hypothetical company, therefore, should resemble a quilt that is constructed of various discrete components (utility patents, design patents, trade secrets, trademarks, service marks, copyright, and IP agreements) that are combined to provide the desired level of IP coverage.

The assertion and defence of patent litigation

The threat of patent litigation

Just a few years ago, patent litigation was ubiquitous. Identifying an unique market opportunity, non-practising entities ("NPEs"), also known as "patent trolls", sprung up, aggregated patents, targeted specific industries, and monetised those patents either through threats of litigation or actual lawsuits. One sector that was the subject of this attack was the telecommunications industry. Beyond a number of competitor-versus-competitor suits (such as *Apple v. Samsung*), large, sophisticated NPEs also arose that did not make a product or sell a service. Rather, they purchased telecom patents, created portfolios, and engaged in litigation campaigns to force companies to pay royalties on those patents. Often, if a NPE had a large enough portfolio, a telecom company would enter into a licence agreement to license that portfolio for a defined period of time, often five years.

In the last few years, patent litigation has waned. Due to Congress's creation of *inter parties review* ("IPR") proceedings, stricter requirements on proving damages, member organisations that acquire patents and offer licences to their members, restrictions on where patent lawsuits may be filed, and new defences that allow patents to be invalidated more easily in the early stages of litigation, patent litigation is no longer the economic opportunity it once was. While competitors still will engage in patent litigation to preserve (or attack) their relative positions in the marketplace, NPEs have found that this changing landscape has made patent litigation financially less rewarding. To be sure, such patent litigation still exists. Indeed, new lawsuits are filed daily. The number and threat of those lawsuits has greatly diminished, however, and the value of patents generally has diminished as well.

Market changes, of course, can create new incentives for initiating patent litigations, and the increased role of blockchain technology is likely to bring about one of those changes. To the extent blockchain technology becomes prevalent, it is likely to result in substantially increased patent litigation, both between competitors and between NPEs and practising companies. The reasons for this potential change are several:

- In a competitive landscape, certain companies – specifically those technology companies solely directed toward creating blockchain products – must use their patents to keep competitors out of the marketplace.
- Blockchain is ushering in a new set of patents, based on new technology, that have not been licensed.
- Blockchain technology will be used in lucrative fields which, by association, will make blockchain patents more valuable.
- Blockchain technology likely will be used as fundamental building blocks, making the technology more valuable and damages more lucrative.

Certainly, NPEs see the opportunity. Eric Spangenburg, a well-known founder of NPEs, has set up "IPwe" to collect and exploit blockchain patents, and Intellectual Ventures, a well-known and well-financed NPE, similarly is seeking to acquire and exploit patents in this area.[12] And our hypothetical transaction platform reflects this opportunity. If our hypothetical company builds blockchain technology into the basic building blocks of its transactions, and its transactions form the basic building blocks of its business, then it stands to reason that the technology underlying those activities has significant value.

Offensive and defensive uses of patent rights

When entering into this new technical field, therefore, it is critical that our hypothetical company understand the patent landscape. Are there so many patents that they create a barrier to entry? Are other companies actively applying for patents? If so, are they doing so to block others or require licensing fees, or are they doing so merely for defensive purposes? Understanding and properly predicting this landscape may be the difference between a successful and a failed endeavour.

Broadly speaking, the strategic use of patent rights can be categorised as offensive or defensive (or a mix of the two). These strategies are discussed in greater detail below.

- *Offensive uses of patent rights*

  From an offensive perspective, the holder of a patent gains the right to exclude others from making, using or selling the invention.[13] An offensive patent holder therefore has the ability to block all others from utilising its patented inventions. In an emerging technical field like blockchain, patent-filers typically have a more open landscape of new solutions to discover and claim. Because of the patent holder's right to exclude, each solution it is able to patent can block competitors from utilising that solution in their own products or services, unless granted permission.

  For our hypothetical company, if the patented technology allows for a more efficient and secure transaction, our hypothetical company may want to exclude others from using that technology, giving the hypothetical company a competitive advantage in the marketplace. If our hypothetical company does not wish to exclude competitors, it may instead allow other companies to use its patented technology, but demand that they pay reasonable royalties for that use, perhaps to help defray research-and-development costs or to create an alternative revenue stream.

  It is not enough, however, for the offensive patent holder to file and receive issued patents. The offensive patent holder must affirmatively enforce its patent rights, and make sure that those patent rights are not encumbered by open source licences, *per* our discussion below in "The impact of open source software", or by FRAND licensing obligations, *per* our discussion below in "The role of industry standards". Enforcement requires monitoring for activities that may infringe the patent holder's claims, demanding

that others halt infringing activities and, if necessary, instituting litigation to halt the activities by and/or receive reasonable compensation for those activities.

Our hypothetical company also may seek to develop income streams from its patent portfolio. By enforcing its patent rights, the offensive patent-holder may force competitors to take and pay for licences. These licences may provide income to the offensive patent-holder as a single lump sum, where the licensee pays for its license upfront, or as a running royalty, where the licensee pays a percentage of the revenue generated by its products in the marketplace.

- *Defensive uses of patent rights*

  Rather than affirmatively asserting patents, the defensive patent-holder uses them as a hedge against other potential claims against it. Thus, in our hypothetical, where the hypothetical company is building a platform and cannot have that platform's use interrupted, the hypothetical company needs to build up as many defences against a claim of patent infringement as possible. By having its own portfolio, our hypothetical company may be able to deter competitors from a lawsuit against it, because that competitor knows that it may face claims against it if it brings a patent infringement action.

  A defensive strategy, if timely performed, also can block others from securing patents that later can be asserted against it. That is, in fact, the precise strategy of Coinbase's patent filings. By filing for as many patents as possible in the blockchain field, Coinbase hopes to take away patent rights from non-practising entities, which they could otherwise assert against Coinbase.[14]

  Ultimately, as blockchain matures, players in the field will tend to take several forms. Patent leaders will emerge, and to avoid mutual destruction, they will enter into cross-licences with each other. Other companies will try to enter the industry without a proper patent portfolio, and may find significant barriers to entry if the patent leaders seek to assert their right to exclude those other companies from using their patented technology. And then there will be companies that simply acquire patents for the purpose of asserting them. They will create transaction costs, but should not bar entry into the marketplace.

* * *

So, for our hypothetical company, it needs to look at the long-term. Is it creating a platform of critical importance, but leaving itself vulnerable to its competitors? Is it fully taking advantage of its hard work and innovation by protecting the original and novel concepts that it created? Will it find itself blocked by aggressive competitors that are aggregating important patents? All of these questions must be addressed at the same time that our hypothetical company is investing in its technological improvements, and seeking to attract entities and (perhaps) developers to join and participate in its newly created blockchain network.

Strategies for limiting patent litigation exposure

The threat of patent litigation in the blockchain field is real. So how can our hypothetical company limit potential liability? There are several steps that it can take:

- **Open source defences**. At a minimum, if a claim is asserted, our hypothetical company needs to consider whether that claim is blocked or barred by open source restrictions. In addition, our company also should be deliberating carefully on its own open source strategy, and how the use of open source software impacts its potential defences and assertion rights.

- **Actively enter into cross-licence agreements**. If our hypothetical company has acquired a significant patent portfolio, then it may want to approach other major players in the blockchain field and seek to enter into cross-licences with those companies. This approach allows companies to compete based on the quality of their product or service, rather than engage in a damaging patent war.
- **Join patent pools**. In certain industries, particularly telecommunications, companies have arisen to help combat NPEs. These companies are membership-based organisations, whereby companies pay a fee for a licence to all patents held by the company. The company's typical approach is to acquire patents, or take licences on patents, for the benefit of its members. The goal of these organisations is to charge a reasonable fee for a licence to a broad-based portfolio.
- **Monitoring patent application and allowed patents**. While there are many blockchain patents and patent applications, they number in the hundreds, not the thousands. As such, if committed, our hypothetical company can review patent applications as they are published (18 months after filing) and when patents issue. Doing so allows a company to identify potentially problematic patents. The downside of such an approach, however, is that such monitoring may become discoverable in a patent litigation, and perhaps can be used as evidence of knowing (wilful) infringement.
- **Consider design arounds where available**. To the extent our hypothetical company identifies potentially problematic patents or applications, an option for it is to "design around" the problematic patent. In other words, our hypothetical company can analyse the particular elements that make up the invention, and eliminate one or more of those elements in its product in order to avoid practising the patent.
- **Be prepared to file IPRs**. If our hypothetical company finds a problematic patent, one option is to file an IPR with the Patent Office to try to invalidate the patent. Our hypothetical company can take that step even if no lawsuit has been filed against it. Deciding to do so requires an assessment of the likelihood that the patent can be invalidated and the cost associated with that process, but that cost will always be substantially less than the cost of patent litigation.
- **Be prepared to attack the patents on *Alice* grounds**. If our hypothetical company ends up in litigation, it still may be able to terminate that litigation early by filing an Alice motion, discussed more fully in the section, "Defensive uses of patent rights", above. The concept of blockchain itself is an abstract idea, and not patentable as such. To have a valid blockchain patent, the claimed idea must identify some technical problem in the field and provide some specific technical solution to that problem. Without providing something sufficiently concrete, our hypothetical company may be able to invalidate the asserted patent early in the litigation process.
- **Assert counterclaims**. As discussed above, it is important for our hypothetical company to acquire its own patent portfolio. If successful in doing that, and if sued by a practising company, our hypothetical company may be able to assert its own claims of patent infringement. Doing so typically makes it easier to resolve a dispute in its early stages.

The impact of open source software

The term "open source software" refers to software that is distributed in source code form. In source code form, the software can be tested, modified, and improved by entities other than the original developer. The term "proprietary" software refers to software that, in

contrast, is distributed in object code form only. The developer of proprietary software protects its source code as a trade secret, and declines to allow others to modify, maintain, or have visibility into its software code base. Proponents of open source software state that the structure fosters the creation of vibrant – and valuable – developer communities, and leads to a common set of well tested, transparent, interoperable software modules upon which the developer community can standardise.

Open source software is ubiquitous in blockchain platforms. The software code bases for Bitcoin,[15] public Ethereum,[16] and Hyperledger,[17] and portions of the software code bases for Enterprise Ethereum[18] and Corda,[19] all consist of open source software. Bitcoin and Ethereum are the leading public blockchain platforms, and Hyperledger, Corda, and Enterprise Ethereum are the "big three" leading commercial, permissioned blockchain platforms.[20] Accordingly, if our hypothetical company wishes to leverage solutions that rely on software from any of these leading platforms, it must consider the impact of the licences that govern this software.

The open source community has developed a number of licences, and these range from: (a) permissive licences, that allow licensees royalty-free and essentially unfettered rights to use, modify, and distribute applicable software and source code;[21] to (b) restrictive, so-called "copyleft" licences, that place significant conditions on modification and distribution of the applicable software and source code. Two open source licences are particularly relevant to our hypothetical company: the General Public License version 3 ("GPLv3"),[22] because this licence (and variants) governs large portions of the Ethereum code base,[23] and the Apache 2.0 licence (the "Apache License"),[24] because this licence governs open source software provided via the Hyperledger, Corda, and Enterprise Ethereum platforms.[25] Each of these licences embodies a "reciprocity" concept that our hypothetical company must consider.

GPLv3 is known as a "strong" copyleft licence. The licence functions as follows: assume a developer is attracted to a software module subject to GPLv3, and incorporates this module into proprietary software that he or she then distributes to others. To the extent the developer's proprietary software is "based on" the GPLv3 code,[26] the developer is required to make his or her proprietary code publicly available in source code form, at no charge, under the terms of GPLv3. This requirement will remove trade secret protection embodied in the proprietary code, as well as the developer's ability under copyright law to control the copying, modification, distribution, and other exploitation of its software.[27] This licence, therefore, has a significant impact on the developer's trade secret and copyright portfolios.

GPLv3 also has a significant impact on the developer's patent portfolio. The licence obligates the developer to grant to all others a royalty-free licence to patents necessary to make, use, or sell the Derivative Code.[28] Finally, simply by distributing GPLv3 code, without modification, the developer agrees to refrain from bringing a patent infringement suit against anyone else using that GPLv3 code.[29] In sum, the structure of GPLv3 reflects a strong "reciprocal" concept: if a developer wishes to incorporate open source software into its code base, it must reciprocate by contributing that code base (and all needed IP rights) back to the community. As noted above, the Ethereum code base is licensed predominantly under GPLv3. Therefore, our hypothetical company should use caution in relying on Ethereum code.

Our hypothetical company should also consider the impact on its IP portfolio of relying on Hyperledger, Corda, and Enterprise Ethereum code. The Apache licence (or an equivalent) governs large portions of these code bases. For our hypothetical company, although the Apache licence has reciprocal features, it is considerably more flexible than GPLv3. The

Apache licence impacts a developer's rights to its software under patent, trade secret, and copyright law in a manner similar to GPLv3;[30] however, these impacts only arise where the developer affirmatively contributes its software to the maintainer of the Apache code at issue. The structure functions with respect to patents as follows: if a patent owner contributes software to an Apache project, the Apache licence restricts the owner from filing a patent infringement claim against any entity based on that entity's use of the contributed software. If the owner does bring such a suit, the owner's licence to the Apache code underlying its contribution terminates.[31] The licence thus has a reciprocal structure: a patent owner cannot benefit from Apache-licensed software while suing to enforce patents that read on its contributions to the Apache software community. If the developer, however, decides not to contribute its code to an Apache project, the developer remains free to incorporate Apache code into its proprietary code base, and commercialise this code without obligation to the Apache open source community. The Apache licence, therefore, provides developers with considerable flexibility.[32]

This flexibility may present strong value to our hypothetical company. It would permit the company, for example, to leverage existing Apache-licensed software from the Hyperledger, Corda, and Enterprise Ethereum code bases in order to develop its new platform and applications, and would give the company full control over whether and to what extent it wishes to encumber its intellectual property portfolio with open source obligations.

Based on the above, it might appear that our hypothetical company would take extreme steps to avoid GPLv3 code (or other strong copyleft code) and would never contribute code to an Apache project. This, however, has not been the case. A number of entities have contributed code under the Apache licence, for example, in order to encourage developers and users to adopt the permissioned commercial network that implements this code.[33] Our hypothetical company will similarly want to consider the potential benefits of seeking to create a vibrant developer and user community using an "open" approach to its intellectual property portfolio, and potentially contributing code under an appropriate open source software licence. In any event, open source software licences and licensing techniques play a key role in blockchain technology, and our hypothetical company will want to carefully consider these licences and techniques in its IP strategy.

The role of industry standards

Background

Industry standards refer to a set of technical specifications that a large number of industry players agree upon to use in their products.[34] Industry players collaboratively develop these technical specifications in a Standards Setting Organization (or "SSO"). Periodically, the SSO will hold meetings where participants, often scientists and engineers, representing industry players will propose and debate differing proposals regarding how a technology should operate. Decisions regarding proposals, and the final technical specifications that stem from them, are reached by consensus by the participants.

Current efforts to standardise blockchain technology

Several organisations have begun standardising a variety of blockchain technologies:

- The International Standards Organization ("ISO") has formed Technical Committee 307 ("ISO/TC 307") to consider blockchain and distributed ledger technologies.[35]
- The Institute of Electrical and Electronics Engineers ("IEEE") has formed two blockchain groups: (1) Project 2418 to develop a standard framework for the use of

blockchain in Internet-of-Things applications;[36] and (2) Project 825 to develop a guide for interoperability of blockchains for energy transaction applications.[37]

- The Blockchain in Transportation Alliance ("BiTA") is focused on the use of blockchain in freight payments, asset history, chain of custody, smart contracts and other related goals.[38]
- Hyperledger is a blockchain standard project and associated code base hosted by the Linux Foundation that focuses on finance, banking, Internet-of-Things and manufacturing.[39]
- The Enterprise Ethereum Alliance recently released an architecture stack designed to provide the basis for an open-source, standards-based specification to advance the adoption of Ethereum solutions for commercial, permissioned networks (referred to as "Enterprise Ethereum").[40]

Advantages and disadvantages of standards

- *Advantages of using and contributing to industry standards*

  There are several advantages to using standards that benefit an industry at-large:

  - **Ensures product compatibility** – With a standard in place, any vendor can develop a product that will be compatible with other products in the industry.
  - **Stronger technology** – Technical specifications created with the input of many industry players tend to result in stronger overall technologies. In theory, the best ideas should emerge from the process and become industry standards that benefit both vendors and consumers.
  - **Shifts competition from the standardised technology to implementation** – Standardisation allows industry players to avoid competition with regard to the standardised technology, and instead shift their focus to developing the best implementation of the remaining technology. Entities that participate in the standard-setting process are obligated to disclose patents that are essential for implementing the standard, and to provide licences to these patents on fair, reasonable, and non-discriminatory terms (so-called "FRAND" terms). These FRAND obligations ensure that all implementers bear the same licensing burden as regards patents essential to the standard.
  - **Greater likelihood of wide adoption** – Approval by many industry players makes the standardised approach a "safer bet" for technology adopters and investors.

  Contributing to SSOs also yields several benefits to individual participants. First, a participating company gains visibility into what comes next in their industry. For example, a software vendor for a syndicated loan blockchain platform could observe the emerging form and content of the blockchain's smart contracts and begin to steer its internal development toward efficiently processing those contracts. Second, a participating company has the opportunity to guide the standardisation process. For example, steering the SSO toward smart contracts that reference cloud-based digital documents would be advantageous for a vendor with a strong cloud-based solution in place.

- *Disadvantages of using and contributing to industry standards*

  There are disadvantages to employing industry standards as well. First, a company loses control over certain aspects of the technology. Instead of developing technology in isolation, our hypothetical company could be at the whim of the industry and its own competitors. Second, a company could develop its own technology that wins

over others' in the marketplace. Good-faith participation in an SSO implies that a company will contribute its best, most valuable ideas to the SSO instead of applying them solely to its own products. But the prize for developing better technology than the SSO's participants, and not contributing it, is alluring: a lucrative monopoly on the best technology. Third, an SSO is less nimble than an individual company because changes to industry standards takes consensus of many parties, which in turn takes time. Finally, by participating in the SSO process, the company will place FRAND obligations on any patents in its portfolio that are essential for purposes of implementing the standard.

Lessons from wireless telecommunications industry standards

Blockchain technology is a relatively new field, and SSOs are only starting to form to develop blockchain standards. Many companies are now deciding whether to join a blockchain SSO or pursue their own solutions. Another technical field, telecommunications, and the history of its standardisation activities, provides a good example of the advantages and disadvantages of pursuing industry standards or deciding to go it alone.

In order for a phone to access a carrier's wireless network, it must know how to communicate with the carrier's network. Telecommunications standards dictate how that communication proceeds. By adhering to the telecommunications standard, a manufacturer can ensure that its phone can operate on any carrier's wireless network that also follows that standard.

In the 1980s, the European "first generation" wireless telecommunications market was fractured by a handful of standards marked by national or regional boundaries. Scandinavia used a standard called "NMT"; Great Britain used "TACS"; Italy used "RTMS" and "TACS"; France used "RC2000" and "NMT"; and Germany used "C-Netz".[41] Using this hodgepodge of telecommunications standards meant that a German's phone would not work during her vacation to France, and an Englishman's phone would not work in Scandinavia.[42] Manufacturers for both phones and network infrastructure were likewise geographically constrained. These manufacturers would typically only research and develop products for specific European regions. What resulted were regional monopolies for those manufacturers, but with low subscriber rates and little opportunity to compete in foreign markets where their technology would be inoperable.[43]

Mindful of these issues with the first generation wireless telecommunications standards, phone and infrastructure manufacturers from around Europe (and indeed around the world) came together to develop a pan-European, "second generation" standard within the European Telecommunications Standards Institute ("ETSI") SSO. These manufacturers sent their best scientists and engineers to ETSI to ensure that this emerging standard would meet wireless subscribers' and carriers' needs. The result of their work was the Global System for Mobile communications ("GSM"), which was the *de facto* wireless standard throughout Europe and parts of the United States from 1992 through 2002. During that period, manufacturers would compete to develop better phones or network equipment, all the while maintaining compliance with the GSM standard. As a result, equipment developed in Sweden or Finland could be sold throughout Europe. This open market brought the price of wireless technology down, increased subscriber bases and, by adoption of a similar approach in the United States, ushered in today's ubiquitous smartphones and wireless networks.

Analogies can be drawn to current trends in blockchain standardisation. Blockchain is based on networks that are large enough – i.e. have enough nodes – to create reliability. As such, interoperability and scalability are important. Standardisation of blockchain elements can be an important tool in achieving those goals. But the standardisation process often involves competing visions. Certain companies will advance one approach, and other

companies will advance a different approach. That advocacy typically is based on a good faith belief, but it also arises from investments that companies make in their technology.

A meaningful standardisation process contains both risk and opportunity for our hypothetical company. No company wants to make the wrong bet and become the Betamax of blockchain technology. Companies therefore need to be thinking hard about the competing standards that are being created and what role they wish to play in that creation. An entirely passive role could result in other thought leaders seizing the marketplace, but too aggressive a role could lead to massive investments that are not adopted by the marketplace as a whole. Ultimately, every company needs to think about the role that they wish to play on that spectrum.

Acknowledgment

Jacob W.S. Schneider

The authors would like to thank Jacob Schneider, partner in Holland & Knight's Boston office, for his contribution to this chapter.

* * *

Endnotes

1. There are a range of other differences between public and permissioned networks as well. For example, a permissioned network can be structured with different consensus rules that reduce the resource requirements (including electricity requirements) needed on a public network such Bitcoin. There are also a range of gradations between fully public and fully private blockchain networks. The Enterprise Ethereum Alliance, for example, is designed to permit operation on a public network, but to restrict the nodes on that public network that receive the data at issue. *See* I. Allison, Enterprise Ethereum Alliance Is Back – And It's Got a Roadmap (May 2, 2018), located at https://www.coindesk.com/enterprise-ethereum-alliance-isnt-dead-got-roadmap-prove/.
2. Nakamoto, Satoshi, *Bitcoin: A Peer-to-Peer Electronic Cash System* (Oct. 31, 2008) (available at https://bitcoin.org/bitcoin.pdf).
3. 2008 is not the earliest disclosure of blockchain-like solutions. *See* Stuart Haber and W. Scott Stornetta (1991) and Bayer, Haber and Stornetta (1992).
4. https://blogs.thomsonreuters.com/answerson/in-rush-for-blockchain-patents-china-pulls-ahead.
5. https://blogs.thomsonreuters.com/answerson/in-rush-for-blockchain-patents-china-pulls-ahead.
6. https://blogs.thomsonreuters.com/answerson/in-rush-for-blockchain-patents-china-pulls-ahead.
7. https://blogs.thomsonreuters.com/answerson/in-rush-for-blockchain-patents-china-pulls-ahead.
8. http://patentvue.com/2018/01/12/blockchain-patent-filings-dominated-by-financial-services-industry.
9. https://www.ibm.com/blockchain.
10. https://www.delltechnologies.com/en-us/perspectives/tags/blockchain.
11. *Alice Corp. v. CLS Bank Int'l*, 134 S. Ct. 2347 (2014).
12. Certain industry participants have been working to place restrictions on key patents, to prevent them from being acquired by NPEs. *See* Michael del Castilloite, Patent Trolls Beware: 40 Firms Join Fight Against Blockchain IP Abuse (March 16, 2017) located at

https://www.coindesk.com/40-blockchain-firms-unite-in-fight-against-patent-trolls/.

13. 35 U.S. Code § 154(a)(1) ("Every patent shall . . . grant to the patentee, his heirs or assigns, of the right to exclude others from making, using, offering for sale, or selling the invention throughout the United States or importing the invention into the United States . . .").
14. https://blog.coinbase.com/how-we-think-about-patents-at-coinbase-26d82b68e7db.
15. *See* http://www.Bitcoin.org.
16. L. Zeug, "Licensing" (September 4, 2016), located at https://github.com/ethereum/wiki/wiki/Licensing.
17. "About Hyperledger," located at https://www.hyperledger.org/about.
18. Enterprise Ethereum Alliance Specification Clears the Path to a Global Blockchain Ecosystem (May 16, 2018), located at https://entethalliance.org/enterprise-ethereum-alliance-specification-clears-path-global-blockchain-ecosystem/.
19. "Contributing to Corda," located at https://github.com/corda/corda/blob/master/CONTRIBUTING.md; Downloads: DemoBench for Corda 3.0, located at https://www.corda.net/downloads/.
20. R. Brown, "Corda: Open Source Community Update" (May 13, 2018) located at https://medium.com/corda/corda-open-source-community-update-f332386b4038.
21. Bitcoin software, for example, is licensed under the permissive, MIT Licence. *See* http://www.Bitcoin.org; https://opensource.org/licenses/MIT.
22. GPLv3 license, located at https://www.gnu.org/licenses/gpl-3.0.en.html.
23. L. Zeug, "Licensing" (September 4, 2016), located at https://github.com/ethereum/wiki/wiki/Licensing. *See, e.g.*, Ethereum-sandbox License, located at https://github.com/ether-camp/ethereum-sandbox/blob/master/LICENSE.txt.
24. Apache 2.0 license, located at https://www.apache.org/licenses/LICENSE-2.0.
25. For Corda, *see* R. Brown, "Corda: Open Source Community Update" (May 13, 2018) located at https://medium.com/corda/corda-open-source-community-update-f332386b4038; "Contributing to Corda," located at https://github.com/corda/corda/blob/master/CONTRIBUTING.md. For Hyperledger, *see* Brian Behlendorf, "Meet Hyperledger: An 'Umbrella' for Open Source Blockchain & Smart Contract Technologies" (September 13, 2016) located at https://www.hyperledger.org/blog/2016/09/13/meet-hyperledger-an-umbrella-for-open-source-blockchain-smart-contract-technologies. Code contributed to the Enterprise Ethereum Alliance is generally made available under an open source license that mirrors the Apache 2.0 license, *see* Enterprise Ethereum Alliance Inc. Intellectual Property Rights Policy, available at https://entethalliance.org/join/.
26. In defining the key term "based on", GPLv3 largely relies on copyright law rules governing derivative works. Courts generally rule that two copyrighted works are distinct (and one is not derivative of the other), if "they can live their own copyright life;" in other words, the test focuses on whether each expression "has an independent economic value and is, in itself, viable." *E.g., Columbia Pictures Indus. v. Krypton Broad. of Birmingham, Inc.*, 259 F.3d 1186, 1192 (9th Cir. 2001); *Lewis Galoob Toys, Inc. v. Nintendo of America, Inc.*, 964 F.2d 965, 969 (9th Cir. 1992).
27. For convenience, the code the developer is required to open-source in this manner is referred to as "Derivative Code".
28. GPLv3, sec. 11 (Patents).
29. GPLv3, sec. 10 (Automatic Licensing of Downstream Recipients).
30. The maintainer of the relevant Apache code at issue, through the Apache Software

Foundation, has the ability to set downstream terms for the contributed software.

31. Apache 2.0, sec. 3 (Grant of Patent License).
32. Our hypothetical company will also need to consider "compatibility" issues between various open source licences. The Hyperledger platform, for example, was unable to assimilate Ethereum code due to incompatibility between the Apache licence and strong copyleft licences, and the resulting need to obtain permissions from copyright owners to "re-license" the Ethereum code at issue. *See* J. Manning, Hyperledger Fails Ethereum Integration Due To Licensing Conflicts (February 3, 2017), located at https://www.ethnews.com/hyperledger-fails-ethereum-integration-due-to-licensing-conflicts; J. Buntinx, Ethereum app Developers may Face Licensing Issues Later on (December 6, 2017), located at https://www.newsbtc.com/2017/12/06/ethereum-app-developers-may-face-licensing-issues-later/.
33. IBM, for example, has contributed code under the Apache licence to the Hyperledger platform, and in turn is providing commercial Blockchain-as-a-Service (BaaS) offerings based on this platform using IBM's cloud infrastructure. *See IBM Blockchain, The Founder's Handbook: Your guide to getting started with Blockchain* (Edition 2.0) located at https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=28014128USEN. Microsoft has similar commercial offerings, based on Azure and the Enterprise Ethereum platform. *See* M. Finley, Getting Started with Ethereum using Azure Blockchain (January 24, 2018), located at https://blogs.msdn.microsoft.com/premier_developer/2018/01/24/getting-started-with-ethereum-using-azure-blockchain/.
34. A simple example is the shape and voltage of a wall power outlet. Because the power outlet is standardised among geographic regions, an appliance maker can ensure that its coffee maker will work (and can be sold) anywhere within a given region.
35. https://www.iso.org/committee/6266604.html.
36. http://standards.ieee.org/develop/project/2418.html.
37. http://standards.ieee.org/develop/project/825.html.
38. https://bita.studio.
39. https://www.hyperledger.org.
40. Enterprise Ethereum Alliance Advances Web 3.0 Era with Public Release of the Enterprise Ethereum Architecture Stack (May 2, 2018), located at https://entethalliance.org/enterprise-ethereum-alliance-advances-web-3-0-era-public-release-enterprise-ethereum-architecture-stack/; https://entethalliance.org/wp-content/uploads/2018/05/EEA-TS-0001-0-v1.00-EEA-Enterprise-Ethereum-Specification-R1.pdf.
41. Funk, Jeffrey L., Global Competition Between and Within Standards: The Case of Mobile Phones at 39 (New York, Palgrave, 2002); Garrard, Garry A., Cellular Communications: Worldwide Market Development (Boston, Artech House, 1998).
42. Gruber, Harald, The Economics of Mobile Telecommunications (Cambridge University Press, 2005) at 35.
43. *Id.*

Joshua Krumholz
Tel: +1 617 573 5820 / Email: Joshua.Krumholz@hklaw.com

Josh Krumholz is a partner in Holland & Knight's Boston office. A trial attorney and the national Practice Group Co-Leader for the firm's Intellectual Property Group, Mr Krumholz focuses primarily upon intellectual property litigation, with a particular focus on patent litigation. His practice covers a variety of technologies and jurisdictions. Mr Krumholz has successfully taken cases to jury verdict in the Eastern District of Texas, Illinois, Massachusetts, New York and New Jersey, among other jurisdictions. Technologies that Mr Krumholz handles include telecommunications, software, hardware, electronics and consumer goods. Mr Krumholz represents leading companies across a range of industries, including Ericsson Inc., T-Mobile, Inc., Verizon Corp., Avaya Inc., Acushnet Company and Hasbro, Inc., among others.

Ieuan G. Mahony
Tel: +1 617 573 5835 / Email: Ieuan.Mahony@hklaw.com

Ieuan Mahony is a partner in Holland & Knight's Boston office. He concentrates his practice in intellectual property (IP) licensing and development, data privacy and security, and information technology (IT). Mr Mahony combines his transactional and compliance work with dispute resolution and litigation matters. His substantial background in transactional and litigation practice areas helps clients receive high-quality advice in the dynamics of reaching an agreement as well as the realities of combating an adversary. Mr Mahony is a member of the firm's three-partner Information Technology Governance Committee.

Brian J. Colandreo
Tel: +1 617 305 2143 / Email: Brian.Colandreo@hklaw.com

Brian Colandreo is a partner in Holland & Knight's Boston office. Mr Colandreo serves as the National Patent Practice Leader and is a member of the Intellectual Property Group. A registered patent attorney, Mr Colandreo focuses his practice on client management, general intellectual property prosecution, transactional work, litigation support, due diligence work, and utility and design patent opinion work. Prior to entering law school, Mr Colandreo worked as a systems/software engineer for Johnson Controls.

Holland & Knight LLP

800 17th Street N.W., Suite 1100, Washington, DC 20006, USA
Tel: +1 202 955 3000 / Fax: +1 202 955 5564 / URL: www.hklaw.com

www.globallegalinsights.com

Other titles in the **Global Legal Insights** series include:

- **Banking Regulation**
- **Bribery & Corruption**
- **Cartels**
- **Corporate Tax**
- **Employment & Labour Law**
- **Energy**
- **Fund Finance**
- **Initial Public Offerings**
- **International Arbitration**
- **Litigation & Dispute Resolution**
- **Merger Control**
- **Mergers & Acquisitions**
- **Pricing & Reimbursement**

Published by: glg global legal group

Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

The Regulatory Concerns Of Crypto Exchange Registration

By **Jennifer Connors, Josias Dewey, Rebecca Leon and David Sofge** (May 3, 2018, 2:40 PM EDT)

Jennifer Connors

Josias Dewey

Coinbase, one of the largest cryptocurrency exchanges, recently approached the U.S. Securities and Exchange Commission about possible licensing as a broker-dealer. If Coinbase decides to register, it will become among the first of the existing cryptocurrency exchanges to be registered with the SEC. This news comes on the heels of a pronouncement by the SEC Division of Trading and Markets, warning that platforms that offer or trade digital assets that are deemed to be securities, including many initial coin offerings, must register as a national securities exchange or otherwise be exempt from such registration.

In consideration of these recent events and pronouncements, other digital asset exchanges should take note of the regulatory concerns and exemptions related to their operations. While it appears that Coinbase's determination is related to its intention to broaden its offering beyond traditional cryptocurrency, the SEC's statement regarding the trading of digital assets leaves little doubt that, in its view, most ICOs will constitute a securities offering. This article provides a brief overview of the registration options available to digital asset platforms and the benefits and restrictions of registration as a national securities exchange, a broker-dealer operating an alternative trading system, or a funding portal.

National Securities Exchange Registration

The SEC's statement concludes that an online trading platform that brings together buyers and sellers of digital assets deemed to be securities would need to be registered with the SEC as a national securities exchange under Section 6 of the Exchange Act, unless it is otherwise exempt from such registration.

The process of registering as a securities exchange is complex, time-consuming and subject to the SEC's determination that such entity is able to comply with all requirements imposed on exchanges, such as enforcing compliance by its members with its rules as well as the federal securities laws. Fundamentally, registered national securities exchanges are self-regulatory organizations and as such (subject to SEC oversight and approval under Section 19(b) of the Exchange Act), an exchange is able to establish its own rules regarding trading, conduct of members, and applicable fees. Additionally, an exchange is responsible for the supervision and compliance of its members with applicable regulations and therefore has an obligation to develop and maintain inspection and disciplinary programs, as well as monitor and conduct appropriate surveillance of the activities of its members. Under the Exchange Act, a national securities exchange must provide fair access to its members. Although it may limit membership through reasonable standards for access, such standards must not be discriminatory. Finally, all members of a national securities exchange must be registered broker-dealers or persons associated with a

registered broker-dealer.

Rebecca Leon

Takeaway: While the foregoing obligations are no doubt significant and onerous, certain business models may favor the application of a national securities exchange model. If a digital asset exchange wishes to register with the SEC as a national securities exchange, it may enjoy its status as an SRO, which allows it to set its own rules and dictate how it wishes to operate. Certain exchanges may find that control over listing fees from issuers will allow an exchange to better sustain its business model. In addition, while an exchange has significant monitoring and supervisory responsibilities relating to its members, increasingly, SROs contract out a significant portion of their regulatory obligations through a regulatory services agreement. Importantly, the exchange would be limited to admitting members who are registered broker-dealers or their associated persons, thus impeding the ability for retail customers or issuers to trade without the use of an intermediary.

Alternative Trading System Registration

David Sofge

Another option for a cryptocurrency exchange is Regulation ATS, which exempts an ATS from registering as a national securities exchange if it registers as a broker-dealer and provides the SEC with certain information regarding its operations on Form ATS. An ATS generally receives and executes orders in securities electronically through its trading system. While exempt from registration as a national securities exchange, a firm relying on Reg ATS (known as a sponsor) remains subject to several regulatory requirements, some of which are required by Reg ATS, and some of which are due to its status as a broker-dealer.

An ATS also has several ongoing reporting requirements. As with registered national securities exchanges, an ATS may be required to provide fair access to the trading system (provided that trading on the ATS reaches certain thresholds). Additionally, the ATS must establish adequate safeguards and procedures to protect subscribers' confidential trading information and make and maintain prescribed books and records. In order to prevent customer and market participant confusion, an ATS is prohibited from using "exchange," or derivations such as the term "stock market," in its name.

In addition to Reg ATS, additional issues may arise from the ATS' registration as a broker-dealer and compliance with all applicable SEC and Financial Industry Regulatory Authority rules under broker-dealer regulation, including, but not limited to:

- ***Customer Protection:*** Under SEC Rule 15c3-3, a broker-dealer must maintain the physical possession or control of all fully paid securities and excess margin securities carried by the broker-dealer for the account of its customers. A common feature underlying cryptocurrency or digital asset exchanges is the use of distributed ledger technology whereby transactions are recorded on a database that is maintained over a public or private network. Broker-dealers need to consider how the use of DLT impacts the receipt, delivery and custody of securities and other assets of their customer's accounts. For example, will ICO tokens, securities or other assets be held in an individual's account (wallet) or will the sponsor of the ATS provide for the custody of these securities and assets with a third-party qualified custodian?

- ***Books and Records:*** Registered broker-dealers must make and maintain current books and records. Specifically, Rules 17a-3 and 17a-4 under the Exchange Act and FINRA Rule 4511 require that broker-dealers preserve certain records for specified periods of time. The use of DLT must be considered as it potentially impacts a broker-dealer's requirements under these rules. For example, certain records must be maintained for a period of time in a prescribed manner (i.e., solely electronic records must be stored in a "write once read many," or WORM, format). How will a digital-asset ATS ensure that the DLT is recording and maintaining such

information in compliance with applicable rules?

- ***Fees:*** To the extent that a subscriber participating on a digital-asset ATS would be subject to any fees or commissions, additional concerns may arise. Regulatory requirements may apply if a subscriber is subject to fees for the management of wallets and keys, onboarding, or commissions or markups for trades placed through the ATS.

- ***Examinations:*** Dangers relating to regulatory examinations may also arise. Potential registrants and regulators are still in the nascent stages of understanding these new technologies and how existing regulations apply. FINRA's current examination module for an ATS may very well be largely inapplicable to a cryptocurrency or digital-asset ATS.

Takeaway: If a cryptocurrency exchange registers as an ATS, it may have less stringent regulatory requirements than it would if it registers as a national securities exchange. However, the cryptocurrency ATS must still consider the regulatory impact of registration as a broker-dealer.

Funding Portal Registration

The Jobs Act exempts certain intermediaries that operate "funding portals" from the requirement to register with the SEC as a broker-dealer. A funding portal is defined as a crowdfunding intermediary that does not (1) offer investment advice or recommendations, (2) solicit purchases, sales or offers to buy the securities offered or displayed on its website or portal, (3) compensate employees, agents or other persons for such solicitation or based on the sale of securities displayed or referenced on its website or portal, (4) hold, manage, possess or otherwise handle investor funds or securities, or (5) engage in such other activities as the commission, by rule, determines appropriate.

A registered funding portal must be a member of FINRA. While the funding portal does not need to register as a broker-dealer, it remains subject to FINRA's and the SEC's examination, enforcement and rulemaking authority. A funding portal is required to, among other things, provide disclosures and investor education materials to investors, take steps to protect the privacy of information collected from investors, and make efforts to ensure that no investor in a 12-month period has purchased crowdfunded securities that, in the aggregate, from all issuers, exceed certain investment limits.

Takeaway: The crowdfunding portal option is clearly the most limited option for a potential registrant. The activity would be limited to the relatively passive listing of ICOs. Moreover, the compensation model for an operator is limited as well as the receipt of transaction-based compensation is prohibited. Nevertheless, this may be an option depending on the business model and potential issuer base of the digital currency platform.

Conclusion

If Coinbase completes this regulatory process and becomes an SEC-registered exchange, it may herald a wave of registration with the SEC. In this event, these exchanges should take note of the regulatory requirements and concerns related to such registration to decide which option fits best with their current and proposed business model.

Jennifer A. Connors is a partner in the New York office of Holland & Knight LLP.

Josias N. Dewey and Rebecca Leon are partners in the firm's Miami office.

David P. Sofge is an attorney in Holland & Knight's Fort Lauderdale, Florida, office.

Holland & Knight

ALERT

Offering Exemptions Available to Companies Issuing ICOs

May 14, 2018

Jennifer A. Connors
Josias N Dewey
Rebecca Leon
David P Sofge

Qualifying for the race

HIGHLIGHTS:

- Issuing an initial coin offering (ICO) is a new and innovative way for companies to infuse capital into their enterprise. However, several regulatory agencies have increased their scrutiny of ICOs, including the U.S. Securities and Exchange Commission (SEC).
- While ICOs represent an exciting new possibility for capital raises, much uncertainty remains with respect to ongoing regulation and therefore compliance with applicable securities laws is needed to ensure a smooth offering. Failure to comply with applicable securities registration and offering requirements can have severe consequences for the issuer and those involved in the offering and may provide investors with a right of rescission.
- This client alert provides a high-level overview of certain offering exemptions available to a company intending to conduct an ICO pursuant to Regulation D, Regulation A-Plus, Regulation CF or Regulation S.

Issuing an initial coin offering (ICO) is a new and innovative way for companies to infuse capital into their enterprise. One survey recently estimated that the average ICO issued in 2017 raised $12.7 million for each issuing company and current data indicates that ICOs issued in 2018 have already surpassed the total amount of funds raised last year. However, several regulatory agencies have increased their scrutiny of ICOs, including the U.S. Securities and Exchange Commission (SEC). According to recent statements by the SEC, most "tokens" or "coins" issued through an ICO are securities and companies issuing ICOs must consider how these offerings implicate the securities

registration requirements of the federal securities laws.

Companies may find relief from the securities registration requirements through one or more of the exempt offering options provided under federal securities laws. This client alert provides a high-level overview of certain offering exemptions available to a company intending to conduct an ICO pursuant to Regulation D, Regulation A-Plus, Regulation CF or Regulation S.

Exemption	Pros	Cons
Reg D 506(b)	• No capital fundraising limit • Relatively limited filing requirements	• **Cannot** solicit/advertise to the public • Generally must limit to accredited investors (self-certified); 35 nonaccredited • Resale limitations • State law requirements
Reg D 506(c)	• No capital fundraising limit • Relatively limited filing requirements	• **Can** solicit/advertise to the public • Must limit to only accredited investors (reasonably verified) • Resale limitations • State law requirements
Reg A-Plus (Tier 1)	• $20 million capital fundraising limit in a 12-month period • No limits on type of investors (can be offered to general public) • No limits on resale	• Qualification by the SEC and the respective states required
Reg A-Plus (Tier 2)	• $50 million capital fundraising limit in a 12-month period • No limits on type of investors (can be offered to general public) • Initial offering exempt from state registration	• SEC qualification only • Ongoing disclosure requirements • State qualification may be required for resales
Reg CF	• No limits on type of investors (can be offered to general public)	• Low capital fundraising limit and limited amount per investor • Increased reporting

		obligations • Resale limitations
Reg S	• No capital fundraising limit	• Increased monitoring to ensure all investors are non-U.S. persons • May be subject to restriction and registration in foreign jurisdictions • Resale limitations

Regulation D

Regulation D provides for two exemptions under Rule 506(b) and Rule 506(c).

Under Rule 506(b), a company conducting an ICO is not subject to any limitation on the amount of money it can raise pursuant to this offering exemption. However, a company may not use general solicitation or advertising to market the offering and must generally limit its sales to financially sophisticated or accredited investors (or up to 35 nonaccredited investors, provided such investors receive certain additional disclosures). Because of the prohibition on solicitation, the company must generally know that such investors are qualified as accredited investors and may rely on the investors' certification of their status to do so.

Under Rule 506(c), a company conducting an ICO is also not subject to any limitations on the amount of money it can raise. Moreover, under this exemption, a company is permitted to broadly solicit and advertise the ICO, provided that all of the investors are accredited investors. Accordingly, the company may not rely solely on such investors' representations, but must take reasonable steps to verify their status as such.

Both Rule 506(b) and Rule 506(c) require companies to file a notice on Form D that includes the names of the company's executive officers and directors and some limited information about the offering. State regulators also have Form D filing requirements. Finally, under both rules, the tokens or coins issued through the ICO would be restricted securities, which cannot be freely resold in a public marketplace for six months or a year.

Takeaway: A Regulation D exempt offering may be enticing for companies planning on issuing an ICO as it affords no limitation on the amount of capital that may be raised and the regulatory filing requirements are relatively minimal. However, companies that are contemplating an ICO through this exemption are limited by the type of investors who may invest in such offering. To this point, the company should consider the feasibility of sourcing sufficient accredited investors as well as the operational burden of ensuring that investors are accredited and adhering to limitations applicable to nonaccredited investors.

Regulation A-Plus

Like Regulation D, a Regulation A (now known as Regulation A-Plus because of the amendments promulgated by the JOBS Act in 2015) may be available through two options. These options are generally available to U.S. or Canadian issuers not currently subject to reporting requirements of the federal securities laws or subject to a "bad actor" disqualification. In both cases, the offering may be made to the general public and, unlike Regulation D, the coins or tokens so issued are not restricted securities.

The first option, a Tier 1 offering, allows a company to raise up to $20 million in any 12-month period. A company conducting an ICO under this exemption must provide investors with an offering circular which must be filed with, and is subject to review and qualification by, the SEC as well as state regulators where the ICO is being conducted. The offering circular should include information about the ICO, describe the use of proceeds and the risks of the ICO and describe selling shareholders, the company's business, management, performance, plans and financial statements. However, after the offering circular has been filed with the SEC and any applicable state regulators, the company has no other ongoing reporting obligations.

The second option, a Tier 2 offering, allows a company to raise up to $50 million in any 12-month period. Like Tier 1 offerings, companies must give investors access to an offering circular and file with the SEC for review and qualification. However, the company does not need to file with any state securities regulator. Unlike Tier 1 offerings, companies offering under Tier 2 are subject to ongoing reporting requirements and must regularly disclose their financial results and file reports with the SEC. Moreover, Tier 2 limits how much individual investors can invest depending on such investors' net worth, which they may self-certify, provided the company has no knowledge that an investor has exceeded such limit. Additionally, while tokens or coins issued under either tier of Regulation A-Plus are not restricted securities, qualification by state regulators (Blue Sky Laws) may be required for secondary trades in Tier 2 issues.

Takeaway: Regulation A-Plus may be attractive for smaller companies issuing an ICO that are looking to raise capital through the offering of tokens or coins while avoiding some of the more burdensome disclosure requirements. Companies can raise a large amount of capital and, unlike under Regulation D, are not limited to certain types of investors. While a company issuing an ICO under this exemption has some initial (and potentially ongoing) reporting obligations, these requirements are not as burdensome as they would be under a public offering regime.

Regulation CF

Under Regulation CF, a company can raise $1.07 million over a 12-month period. Certain companies are not eligible to use this offering exemption, such as non-U.S. companies, Exchange Act reporting companies, certain investment companies and others. Further, Regulation CF limits how much individuals can invest depending on their net worth. The entire Regulation CF offering must be conducted through an online intermediary registered with the SEC as a funding portal or broker-dealer. The company may not advertise the terms of the offering, except in a limited notice directing potential investors to the registered online intermediary. However, the company can, through the registered online intermediary, communicate with investors regarding the terms of the ICO. Finally, tokens or coins issued in an ICO cannot be resold in public markets within a one-year period.

A company conducting a Regulation CF offering must file an Offering Statement Disclosure via Form C with the SEC, which discloses certain information about the company and its business. Furthermore, a company that offers securities through Regulation CF has a continued reporting obligation and must provide an annual report that contains certain information about the company.

Takeaway: Regulation CF provides for the lowest capital amount and imposes heightened reporting obligations on a company issuing an ICO. Furthermore, while there are no restrictions on the type of investors, these investors are more limited in how much they can invest compared to the limits established in Regulation A-Plus.Nevertheless, this exemption does provide a fundraising avenue to many small companies that may have previously turned exclusively to friends and family or utilized bank loans.

Regulation S

Another potential avenue for companies is to engage in a purely offshore offering to non-U.S. persons pursuant to Regulation S. It should be noted however, that companies relying upon this offering exemption must take several steps to ensure that potential investors are indeed non-U.S. persons and take steps to ensure that securities are not offered into the U.S. without registration. Moreover, companies need to be aware of the offering restrictions and registration requirements of the various countries in which their investors reside, thus creating a complex task for an issuer seeking to take advantage of this exemption. In addition, similar to the other offering exemptions, resales using the public markets in the U.S. are not permitted unless a seller uses another applicable offering exemption.

Takeaway: In addition to enforcing restrictions on sales to U.S. persons, a company seeking to conduct an ICO through Regulation S must ensure that it is knowledgeable about the offering restrictions in the countries in which non-U.S. investors reside to avoid adverse regulatory action and/or rescission by such investors.

Conclusion

While ICOs represent an exciting new possibility for capital raises, much uncertainty remains with respect to ongoing regulation and therefore compliance with applicable securities laws is needed to ensure a smooth offering. Depending on a company's goals and tolerance for associated regulatory burdens, the company may have a strong preference for a certain form of exempt offering. These offering exemptions provide a "middle ground" for a company looking to raise capital when compared to other capital raising initiatives, such as offerings to private equity firms, venture capital firms and public offerings under the federal securities laws.

Clients with questions regarding exemptions for companies issuing ICOs, may contact Jennifer Connors, Josias Dewey, Rebecca Leon or David Sofge.

Authors

Jennifer Connors is a New York financial services attorney who represents broker-dealers, alternative trading systems (ATSs), financial technology (FinTech) companies and other market participants on securities law and market regulation matters. Ms. Connors' practice has a particular emphasis on broker-dealer regulation and compliance issues, trading rules, issues regarding ATSs, electronic trading, cybersecurity, sales practices and anti-money laundering (AML) rules. She also advises FinTech companies and fund management clients with respect to broker-dealer regulation issues, as well as securities offerings and private placements.
212.513.3443 | Jennifer.Connors@hklaw.com

Josias "Joe" N. Dewey is a financial services and real estate attorney and is considered a thought leader on blockchain and distributed ledger technology (DLT). Mr. Dewey is the co-author of the book, "The Blockchain: A Guide for Legal and Business Professionals," published by Thomson Reuters. Mr. Dewey formally served as the leader of Holland & Knight's Miami Real Estate practice group.
305.789.7746 | joe.dewey@hklaw.com

Rebecca Leon is a financial services regulatory attorney in Holland & Knight's Miami office, and a member of the firm's Financial Services Team. Ms. Leon advises broker-dealers, investment advisers, fund managers, banks and other wealth managers on a variety of U.S. and international regulatory and operational matters.
305.789.7703 | Rebecca.Leon@hklaw.com

David Sofge is an attorney in Holland & Knight's Fort Lauderdale office. He represents public and private companies in corporate and financing transactions and regulatory compliance.
954.468.7884 | David.Sofge@hklaw.com

What IP Practitioners Should Know About Blockchain

Joshua Krumholz

April 5, 2019

Holland & Knight

#57876739

Summary of Topics

- Patenting Blockchain Concepts
- The Role and Impact of Open Source Software
- The Threat of Litigation
- Lessons from Telecom Standards

Patenting Blockchain Concepts – Blockchain Basics Are Not Patentable

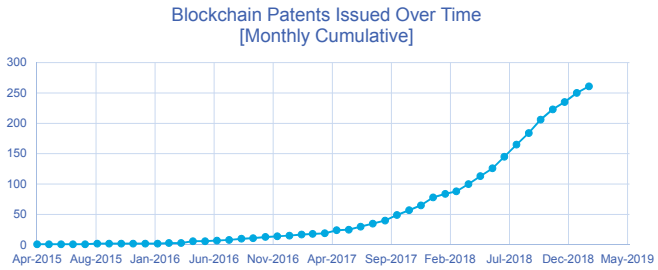
- The creator of blockchain, under the pseudonym Satoshi Nakamota, dedicated his basic concepts to the public in 2008, making them unpatentable
- Many blockchain concepts are unpatentable abstract ideas under *Alice*
- The absence of foundational patents may have sped up development
- Ideas implementing blockchain technology can be patentable

Patenting Blockchain Concepts – Many Potential Applications

- There are a large number of potential applications that could lead to patentable ideas
- Examples include the HSBC's new blockchain platform, JP Morgan's JP Coin, the Boomerang Project, Tari Tickets and the Codex Project
- Challenges that could be overcome by blockchain include –
  - Safely and securely transferring medical records
  - Addressing counterfeit drugs
  - Tracking food from farm to table

Patenting Blockchain Concepts – Applications and Allowed Patents

- The PTO has allowed over 260 blockchain-related patents, up from 2 in 2015 to 170 in 2018
- Over 1,500 patent applications are pending
- Chinese companies account for a significant number of applications



Patenting Blockchain Concepts – Examples of Allowed Patents

- U.S. Patent No. 10,055,446 – Ensuring Data Integrity of Executed Transactions
- U.S. Patent No. 9,875,510 – Consensus System for Tracking Peer-to-Peer Digital Records
- U.S. Patent No. 9,807,106 – Mitigating Blockchain Attacks

The Role and Impact of Open Source Software

- Open source software – Software that is distributed in source code form and available for use by anyone to test, modify and use. Open source source code is unrestricted
- Proprietary software – Software that is distributed in object code only. The source code is protected as a trade secret, and cannot be modified without permission of the developer

The Role and Impact of Open Source Software – Public and Permissioned Networks

- Public networks (Ethereum, Bitcoin) – Nodes are anonymous and each node contains all transactions
- Permissioned networks (Enterprise Ethereum, Hyperledger, Corda) – Network members are vetted and approved, the nodes are not anonymous, and transactional information can be selectively disclosed
- Business networks typically are permissioned networks, and that is especially the case for businesses that are regulated, like financial institutions

The Role and Impact of Open Source Software – Networks Use Open Source Software

- Blockchain networks are based on open source software
- The General Public License, version 3 ("GPLv3") governs large portions of the Ethereum code base
- The Apache 2.0 license ("Apache") governs open source software used for Hyperledger, Corda and Enterprise Ethereum
- The rights and duties of the users of the above networks may be substantially impacted by these open source licenses

The Role and Impact of Open Source Software – GPLv3 and Apache Terms

- GPLv3 license (Ethereum)
  - Strong "copyleft" license
  - If a developer incorporates GPLv3 code into his/her proprietary code, the developer must make that proprietary code publicly available and royalty-free, including a royalty-free license for patents that cover the code (to the extent necessary to use the code)
- Apache license (Hyperledger, Corda and Enterprise Etherium)
  - Apache is more flexible that GPLv3
  - Using the software is not enough to restrict rights; the developer needs to affirmatively contribute the proprietary code to the network for restrictions to apply
  - The restrictions are similar to GPLv3, except that the developer can sue for patent infringement, but then loses the right to use the Apache code

The Role and Impact of Open Source Software – Making Conscious Choices

- The foregoing would suggest that developers stay away from Hyperledger, but in fact IBM and Microsoft have made significant contributions to that code base
- The important lesson is to make sure that developers are not choosing the code base to use without input from legal, otherwise they may be unintentionally giving away the company's IP rights

The Threat of Litigation Generally

- As a highly disruptive technology, blockchain has the potential of drawing significant litigation
- Examples include:
  - Fraud cases, which presently are the vast majority of cases
  - Litigation brought by threatened stakeholders
  - Litigation brought by blockchain partners
- Blockchain implementers need to consider carefully
  - The impact of the change on stakeholders and whether any exposure exists
  - The terms and agreements they have with their blockchain partners

The Threat of Patent Litigation – Blockchain as a Potential New Wave of Litigation

- In recent years, the threat of patent litigation has waned due to changes in the law and the market
- Blockchain may cause an increase of patent litigation because:
  - A competitive landscape may cause companies to use their patents as a sword
  - There are many new patents that have not yet been licensed
  - Blockchain technology is being used in lucrative fields
  - Blockchain technology will likely be used as fundamental building blocks
- Trolls are already getting themselves ready
  - And failed startups may become trolls down the line

The Threat of Patent Litigation – Pre-Litigation Strategies

- Cross-licensing. The companies with the largest portfolios will cross-license with each other
- Patent pools. License-based organizations that accumulate patents to take them off the market are already being formed in this field
- Monitoring patent applications and issuances. Monitoring is doable given the volume but may come with some risk of establishing willfulness
- Design-arounds. It is easier to avoid a patent during the design phase than to try to change the product after launch
- IPRs. *Inter Partes* Reviews can be filed before litigation

The Threat of Patent Litigation – Strategies Once You Are in Litigation

- IPRs. IPRs can be filed up to one year from the filing of the lawsuit
- Open source defenses. Open source restrictions follow a patent after transfer, so should be considered in any defense strategy
- Attacking on *Alice* grounds. Concept patents should not be allowed, but sometimes they are and are vulnerable to attack
- Asserting counterclaims. You need to assess the extent to which you can use your portfolio to assert patent infringement against the plaintiff

The Threat of Patent Litigation – Patent Pledges

- Unilateral patent pledges – Coinbase and Blockstream have pledged to use blockchain patents only for defensive purposes
- Multilateral patent pledges – Members of an organization agree not to sue each other. Examples include DPL, LoT and OIN
- Challenging approach and done by companies that probably would cross-license anyway

Lessons From Telecom Standards – Creating Blockchain Standards

- Standards could help with blockchain scalability
- Standards efforts are already underway
  - Blockchain in Transportation Alliance (BiTA)
  - International Standards Organization (ISO)
  - Institute of Electrical and Electronics Engineers (IEEE)
- To participate or not to participate in standards creation
  - Pros: Helping to shape the future, staying up to date on developments, avoiding being the Betamax of blockchain
  - Cons: It is a major investment and commitment, and you still may end up as the Betamax of blockchain

Lessons from Telecom Standards – Challenges

- Because blockchain potentially covers so many industries, it may be hard to get consensus on what technology to standardize
- Standards lead to standard-essential patents, which can exacerbate patent litigation threats
- Establishing FRAND (fair, reasonable and nondiscriminatory) terms with so many different industries could be challenging