

# Intellectual Property Issues in Blockchain and FinTech

December 2018

FinTech

---

[FinTech](#) refers to the use of new and emerging technologies in the financial services industry to improve the delivery of financial services to customers, and includes innovations such as cryptocurrencies and open banking. Recent years have ushered in the use of several key technologies in the FinTech landscape, including artificial intelligence, data analytics, and blockchain and other distributed ledger technologies. Since the Bitcoin [whitepaper](#) was released in [2008](#) and the Bitcoin blockchain was first implemented in [2009](#), blockchain has gained prominence as an innovative distributed ledger technology that has the potential for [widespread](#) use across a number of industries, including financial services, energy, health care, transportation, and cybersecurity.

As its name implies, blockchain refers to a chain of digital records that are timestamped and organized into blocks, where each block is added in a sequential manner and linked through a cryptographic “hash” of information contained in the prior block in the chain. Each block is stored in a distributed ledger, which is shared, replicated, and synchronized among the participating nodes of a decentralized peer-to-peer network where each such node adheres to a set of rules for validating the addition of blocks to the chain. This characteristic is said to result in an immutable ledger of transactions that cannot be edited or deleted, thereby making a blockchain secure by design.

Since many blockchain technologies establish ownership via a decentralized ledger and also eliminate the need for an intermediary to process transactions, blockchain transactions may have lower [fees](#) and thereby pose a competitive challenge to traditional payment systems. [Blockchain networks](#) are already being used in connection with global payments, asset management, smart contracts, supply chain management, and digital identity.

## Intellectual Property Considerations

According to one [report](#) by an intellectual property (IP) analytics company, while large banks have invested in FinTech and have obtained patents in areas such as online and mobile banking and e-commerce, there are several “traditional” technology companies that *each* have obtained more FinTech patents than all of the banks combined. Banks recognize blockchain as both an opportunity and potentially as a disruptive threat. Accordingly, the report also indicates that banks and other financial institutions are obtaining blockchain related patents at a similar or higher rate than technology companies.

The IP team at Covington understands the disruptive technologies and legal issues that are pertinent to the financial services industry, and provides clients with targeted advice in areas of patent, trademark, copyright, and trade secret law. Covington regularly supports financial institutions, large global technology companies, and startups on the development and implementation of domestic and global strategies that protect technology and secure IP rights.

Given the pace at which technology continues to disrupt the financial services industry, securing IP assets—especially patents—should be a primary consideration for companies in the FinTech space. As the FinTech landscape continues to evolve into areas such as artificial intelligence and machine learning, quantum computing, and big data, a number of important issues should be analyzed by counsel with specialized knowledge and experience in devising IP strategies that align with business objectives, as explained below.

## Patents

A U.S. patent provides the right to exclude others from [making](#), using, offering for sale, or selling a claimed invention within the U.S., or importing the invention into the U.S., for up to 20 years from the effective filing date. Patent rights are considered by many companies to be a core component of their IP and broader business strategies.

### Section §101 and Patent Eligibility

By [statute](#), patents protect *useful* inventions, not mere “abstract ideas.” Recent U.S. Supreme Court decisions have provided an analytical framework that often makes it difficult for courts to determine whether an invention is eligible for patent protection, or whether it might instead be directed to a patent-ineligible abstract idea. And with courts striking down many so-called “business method” patents as being patent-ineligible, determining how to disclose and claim inventions and obtain patents that are able to withstand subject matter eligibility challenges have become critical issues.

In 2014, a renewed focus on the issue of patent eligibility for computer-implemented inventions was instigated by the Supreme Court’s *Alice* [decision](#), which set forth a two-step eligibility test. If an invention is directed to a patent-ineligible abstract idea under the first step, the second step determines whether the patent’s claim(s) (which places the public on notice of the scope of the patentee’s right to exclude) recites elements that transform the abstract idea into a patent-eligible invention.

Courts have generally applied this test to determine that the mere use of commercially available computing devices and software to implement an abstract concept is ineligible for patent protection. For instance, the use of a standard computer system to implement an escrow service for financial transactions was deemed in the *Alice* case to be ineligible for patent protection. However, a court might determine that the use of an innovative database technology to more efficiently conduct various aspects of financial transactions could transform abstract ideas relating to financial transactions into a patent eligible invention. While it is difficult to [predict](#) with certainty whether an invention may be patent eligible, conferring with patent counsel is critical for obtaining guidance that will allow a well-informed decision to be made.

### Divided Infringement

A patented method claim recites a series of acts, or “steps,” to be performed, and patent infringement occurs when all recited steps are attributable to a particular party. If you suspect that a competitor is infringing your patented method, a “divided infringement” problem arises when it turns out that only *some* of the claimed method steps are performed by your competitor, but other steps are performed by a different entity, such as a competitor’s customer, as shown below:

1. A method for use in a communication system

- Step A: analyzing data at a cell tower...
  - Step B: estimating a value of the data...
  - Step C: transmitting the value from the tower...
  - Step D: receiving the value at a mobile device...
- 
- The diagram uses brackets to group the steps. A pink bracket on the right side groups Steps A, B, and C, with the text "Performed by Competitor (e.g., service provider)" next to it. A green bracket on the right side groups Step D, with the text "Performed by another party (e.g., customer)" next to it.

In some circumstances, [courts](#) have *attributed the performance* of Step D (above) to the competitor on the basis that the competitor *directed or controlled* the performance of the other party. Divided infringement issues can be avoided by drafting claims that capture the activity of a single entity, such as a competitor.

For example, although different entities may be involved in conducting transactions in a blockchain, patent claims should ideally be drafted so all steps are performed by a single network entity. For a private blockchain, this could be the managing entity that implements and enforces rules for validating the integrity of new blocks of data before they are added to the ledger. While courts will inevitably be confronted with FinTech innovations posing unforeseen legal and factual circumstances, drafting patent claims from the perspective of a single actor may simplify the task of a patent owner to show infringement and to monetize or otherwise enjoy the patent.

### Extraterritoriality

The patent [statute](#) generally limits the territorial reach of U.S. patents. Thus, systems having components in different geographical regions raises the question of *where* the act of patent infringement occurs.

The answer may depend on whether the patent claim is to a *method* (reciting steps to be performed, as discussed above), or to a *system* or *device* (reciting interrelated structural elements or components). For a claimed [method](#), an infringing use requires *all* recited steps to be performed in the U.S. However, for a claimed system, an infringing use is the place where “control” of the system is exercised and its “benefits” are obtained, which may be in the U.S. even if some of the claimed components are located outside of the U.S.

Under certain circumstances, claims can be drafted to capture U.S.-based activity or systems in a manner that takes into account and potentially avoids extraterritoriality issues. On the other hand, FinTech transactions often involve cross-border activity—for example, a currency trading platform spanning international boundaries. As such, the geographic location of each component of your competitor’s system must be taken into account when considering U.S. claim drafting strategy.

A comprehensive IP strategy should consider patent protection in countries that are relevant to particular business strategies, and how patent protection can encompass cross-border activities in such countries. Having patent counsel that can assess extraterritoriality considerations is of paramount importance in devising an IP strategy that provides an appropriate scope of patent protection.

### **Trade Secrets**

As an alternative to obtaining a patent, a company may maintain confidential information that provides an economic advantage over competitors as a *trade secret*. While patent law is premised on granting a *temporary* right to exclude others in exchange for the *public disclosure* of an invention, trade secret law provides an avenue for obtaining potentially *perpetual*

protection for economically valuable information such as a formula or algorithm. Two well-known examples of trade secrets are the formula for Coca-Cola and the search engine algorithm used by Google.

Trade secret protection, however, presents its own set of issues. If a trade secret holder fails to maintain secrecy or if the information is independently discovered, becomes released or otherwise becomes generally known, protection as a trade secret is lost. In fact, the subject of a trade secret may be patented by someone else who independently developed the trade secret. Covington's IP team is experienced in assisting clients with weighing the relevant considerations in determining an appropriate balance of patent and trade secret protection.

### **Open Source and Standardization**

Open source software, for which the code is freely used, modified, and shared pursuant to [licenses](#), is used by a wide variety of technology [companies](#). In the blockchain space, for example, the software underlying the [Bitcoin](#) and [Ethereum](#) ledgers is open source. While the software itself is freely accessible, obtaining patent protection for inventions that use open source software is possible where the technical improvements satisfy the patent eligibility requirements, such as being novel and not obvious over prior art.

Similarly, companies that engage in developing industry standards have historically been active in acquiring patents. For example, various features of wireless networks that were adopted by [standards setting organizations](#) did not preclude the issuance and proliferation of a wide variety of wireless network [patents](#). However, patents obtained in this context may be subject to [licensing](#) commitments; members of a standards setting organization typically [agree](#) to license, on fair, reasonable, and non-discriminatory terms, inventions that are "essential" to (i.e., must be used to comply with) the technical standard. Thus, FinTech companies should consider a multiplicity of issues that pertain to the use of open source software, industry [standards](#), and licensing of IP rights in consultation with counsel during the course of developing an IP strategy.

If you have any questions concerning the material discussed in this document, please contact the following lawyers:

<a href="#">Michael Nonaka</a>	+1 202 662 5727	<a href="mailto:mnonaka@cov.com">mnonaka@cov.com</a>
<a href="#">Burr Eckstut</a>	+1 212 841 1112	<a href="mailto:beckstut@cov.com">beckstut@cov.com</a>
<a href="#">Gregory Discher</a>	+1 202 662 5485	<a href="mailto:gdischer@cov.com">gdischer@cov.com</a>
<a href="#">David Stein</a>	+1 202 662 5074	<a href="mailto:dstein@cov.com">dstein@cov.com</a>
<a href="#">Raj Paul</a>	+1 202 662 5740	<a href="mailto:rpaul@cov.com">rpaul@cov.com</a>

This information is not intended as legal advice. Readers should seek specific legal advice before acting with regard to the subjects mentioned herein.

Covington & Burling LLP, an international law firm, provides corporate, litigation and regulatory expertise to enable clients to achieve their goals. This communication is intended to bring relevant developments to our clients and other interested colleagues. Please send an email to [unsubscribe@cov.com](mailto:unsubscribe@cov.com) if you do not wish to receive future emails or electronic alerts.