SheppardMullin

Patent Strategies for Cryptocurrencies and Blockchain Technology

Cryptocurrencies and blockchain technology are rapidly emerging as disruptive technologies. As has happened with many new technologies, particularly disruptive ones, a patent arms race is occurring. The number of patents being filed for these technologies is rapidly increasing.

Based on a recent search of the U.S. Patent and Trademark Office database, using sample keywords shown below, it is clear that, while relatively few patents have been issued to date, a flurry of activity is occurring. The number of published applications shows roughly a tenfold increase over the number of issued patents. Note that patent applications are published 18 months after they are filed. This means that the number of pending applications is likely much greater than what is shown below.

Number of Hits By Keyword

Keyword	Issued U.S. Patents	Published Applications
blockchain	61	522
cryptocurrency	55	373
bitcoin	279	1126
Ethereum	6	74
distributed ledger	7	204
smart contract	11	160

Numbers current as of 1-12-18 based on search at USPTO.gov

Despite this increase in patent filing activity, many companies are unaware of what aspects of this technology can be patented and many myths and misconceptions exist. In addition to the usual misconceptions about patents (detailed below), the open source aspect of many blockchain-based inventions leads to greater confusion. The patentability of software and technology platforms does not cease just because some or all of the software is open source or built on a known protocol.

This paper addresses what companies need to know about patent strategies for cryptocurrencies and blockchain technology. The key takeaway is to consult with a patent attorney who focuses on blockchain technology and get an assessment of whether your inventions are patentable. Don't miss out due to misconceptions or bad advice.

Overview

It is not the purpose of this paper to explore the pros and cons of cryptocurrencies and blockchain technology, but a brief overview will be provided to address some of the terminology used in this paper.

Cryptocurrencies are a form of digital currency that use cryptography to enable payments transfers between two parties without the involvement of a third party. Popular examples include Bitcoin and Ethereum. Well over a thousand other cryptocurrencies exist, many having unique functions and protocols. Bitcoin is primarily just a digital currency and is based on a whitepaper entitled "Bitcoin: A Peer-to-Peer Electronic Cash System." Ethereum is a digital currency, but is programmable to enable additional functionality. It is based on a whitepaper entitled "A Next-Generation Smart Contract and Decentralized Application Platform."

Smart contracts are self-executing contracts. Simply put, they are contracts expressed and implemented in computer code stored and running on a blockchain. No lawyers, judges or juries are needed to enforce the contract, because the terms are self-executing via the computer code. Smart contracts are attributed to Nick Szabo based on a pair of papers entitled "Smart Contracts: Building Blocks for Digital Free Markets" and "Formalizing and Securing Relationships on Public Networks"

Blockchain is a technology distinct from cryptocurrencies. It is a decentralized database, commonly referred to as a distributed ledger. Blockchain is one type of distributed ledger. It is a technology for recording transactions. The transactions can include cryptocurrency transactions, but can include other types of transactions including title recordation, voting, digital escrows, to name just a few. Many types of blockchains exist and many more will be built. Blockchains can be public or private.

Some cryptocurrencies operate without a blockchain. One of the leading ones is IOTA, which uses the Tangle ledger, which offers high scalability, no fee transactions, and machine-to-machine transactions. It was designed to provide a commerce capability for the Internet of Things (IoT), with devices transacting directly with other devices.

One reason these technologies are disruptive is that they disintermediate much of the existing financial and payment system. Cryptocurrencies are typically peer-to-peer (P2P) payments. Cryptocurrencies originally started as a libertarian movement, but have recently received support from many enterprise players, including banks, credit card companies, digital payment processors, major technology players and many more. The use of cryptocurrencies and blockchain technology is not limited to the financial world and financial transactions. Blockchain-based transactions can and will be leveraged by every industry.

There is great debate about whether the rapid increase in cryptocurrency prices is a bubble. Regardless of how this plays out, there seems to be little debate that blockchain technology has a very promising future for certain applications. Commercial entities are just starting to build out applications and smart contracts that leverage this technology. Many others are studying the space with great interest. Historically, when this phase of commercial adoption occurs, a rapid increase in patent filings often follows.

The transformative impact of the internet serves as a useful analogy for the potential of cryptocurrencies and blockchain technology. At its core, the internet is based on the TCP/IP, a data communication protocol. It specifies how data is exchanged over the internet by providing end-to-end communications that identify how it should be broken into packets, addressed, transmitted, routed and received at the destination. Many technologies have been built to leverage and improve the use of this protocol. Many of these technologies and applications have been patented.

A similar situation exists with blockchain technology. Various types of blockchains exist, but at its core blockchain technology specifies a transaction protocol. It typically specifies how transactions are implemented, verified and recorded. Many technologies will be built to leverage and improve the use of these protocols and many applications have been and will be built on top of these protocols. Many of these applications have been and will be patented.

As transformative as the internet was, the potential for cryptocurrencies and blockchain technology may be even greater. Significant investments are being made to invent new and disruptive technologies in these areas. Patent protection needs to be considered to protect these investments.

Overview of Patentability

Patents are without a doubt the most misunderstood form of IP protection. We have frequently heard people say you cannot patent software or business methods. This is a gross over-generalization and leads to many missed opportunities for those who hold this belief. Recent cases have redefined what is patentable in the United States, but there is no *per se* prohibition on patenting software or business methods, assuming the criteria for patentability are met. This has become harder recently, but the opportunity still exists.

Cryptocurrency and blockchain technology are basically software running on a computer platform. Other applications of software and technology platforms are patentable and are frequently patented. Yet, many overlook this fact and forego patent protection.

Broadly speaking, patents are available for the software and technology aspects of cryptocurrency and blockchain, and applications of this technology (assuming the criteria for patentability are met).

The primary criteria for patentable subject matter in the United States is that the invention must be for a new and useful process or machine.[1] The subject matter must not be merely an abstract idea, law of nature or natural phenomena. Assuming the subject matter qualifies for patent protection, it must also be non-obvious (which is determined by a legal test).

[1] For completeness, articles of manufacture and composition of matter are also patent eligible, but likely less relevant here.

Putting legal jargon aside, if you have built new and useful technology, that does something that has not been done before or that does something already known in a more efficient way, or an application that leverages such technology, you should consult with a patent attorney to consider patent protection.

Utility Patents Versus Design Patents

Utility patents cover various features, functions and processes relating to cryptocurrencies, blockchain technology and the technological components of the platforms associated with them. Patents also are available for the applications that leverage new cryptocurrency and blockchain technologies to implement innovative services and business methods.

Design patents can be obtained for the ornamental design of a functional item, but not the functionality itself. Various aspects of computer displays, icons and user interfaces can be covered with design patents. Cameron Winklevoss obtained a design patent (D759,073) for a display screen portion of a graphical user interface for presenting cryptocurrency information.

Categories of Cryptocurrency and Blockchain Patents

At a high level, it can be useful to look at inventions as core technologies and applications of technology. The following is a non-exhaustive list of examples.

Examples of Potentially Patentable Core Technologies

- Blockchain technology, distributed ledgers, storage, data structures
- Transaction protocols, processing and validation methods
- Security
- Digital wallets
- Smart contract platforms
- Exchanges
- Mining
- Consensus methodologies
- Merchant services
- Ledger data mining and analysis

Examples of Potentially Patentable Applications

- Functionally unique currencies and tokens
- Payment applications – POS, P2P, remittances
- Lending – P2P, microlending
- E-commerce, micropayments
- Smart Contract Applications
- Decentralized Storage
- Identity Management
- Securities Markets and Services
- Shareholder Management, Share Registries
- Crowdfunding
- Title Systems, IP Rights, DRM, Royalty tracking and payments
- Voting Systems
- Digital Escrows
- Data Analytics
- Supply Chain
- Loyalty Programs
- IoT applications leveraging blockchain
- Health Records
- Energy and Utilities Applications
- Games, Gaming and Wagering
- DAOs and Dapps
- And much more

Some examples of patents already issued for cryptocurrency and blockchain technologies include the following[2]:

Computer Access Control and Authentication

U.S. Patent No. 9,858,781 (issued to Tyco Integrated Security, LLC on January 2, 2018) relates to using a distributed ledger to control connections/access between a facility (e.g., a secured network of computers) and a user device. The distributed ledger stores facility public keys and user public keys. A facility can validate a user using a user's public key and a user device can validate the facility using the facility's public key.

U.S. Patent No. 9,853,977 (issued to Winklevoss IP, LLC on December 26, 2017) relates to authenticating a user based on trusted and distributed authentication servers.

Document Verification

U.S. Patent No. 9,853,819 (issued to Guardtime IP Holdings Ltd. on December 26, 2017) relates to validating a digital document, including an ability to identify each entity involved in registering the digital document by storing document validation information and entity information on a blockchain.

U.S. Patent No. 9,842,216 (issued to NewVoiceMedia, Ltd. on December 12, 2017) relates to generating tamper-proof timestamps on a blockchain and using the timestamps to encrypt communication recordings.

U.S. Patent No. 9,855,785 (issued to UIPCO, LLC on January 2, 2018) relates to generating digital seals for document verification, which may be stored on a distributed ledger.

Identity Management

U.S. Patent No. 9,635,000 (issued to Sead Muftic on April 25, 2017) relates to an identity management system (IDMS) based on the concept of peer-to-peer protocols and the public identities ledger.

Voting Systems

U.S. Patent No. 9,836,908 (issued to Blockchain Technologies Corporation on December 5, 2017) relates to securely storing votes digitally signed by voters on a blockchain.

[2] The brief summary is an overview of what the patent relates to not an opinion on the precise legal scope of protection

Identifying Users in Pseudonymous Transactions

U.S. Patent No. 9,298,806 (issued to Coinlab, Inc. on March 29, 2016) relates to a system configured for analyzing transactions in a distributed ledger to de-anonymize transactions. The system identifies transactions where addresses and/or groupings of addresses are co-spent together and determine whether the addresses and/or groupings of addresses should be associated with each other.

U.S. Patent No. 9,825,931 (issued to Bank Of America Corporation on November 21, 2017) relates to building and updating a distributed ledger that stores real-time identification information including an initial identification of the user. Subsequent identifications are stored and changes or morphs in identification, such as signatures, physical attributes, or locations of the user are identified. User facts are correlated with the identifications to build a timeline for the user.

U.S. Patent No. 9,830,593 (issued to SS8 Networks, Inc. on November 28, 2017) relates to building and updating a blockchain that stores key-addresses (e.g., public keys) of users and identifying information (e.g., IP addresses) involved in cryptocurrency transactions and identifying users in those cryptocurrency transactions based on the blockchain. Identifying information may be further obtained by parsing online communications that relays the user's public key (e.g., emails, chats, etc., that ask for payment and include a user's public key to process those payments) and associating the online communications with IP addresses.

Blocking Payments in Non-Sanctioned Pseudonymous Transactions

U.S. Patent No. 9,852,427 (issued to IDM Global, Inc. on December 26, 2017) relates to verifying whether cryptocurrency transactions should be blocked based on previously stored transaction information that indicates fraudulent or non-sanctioned (e.g., money laundering) activity.

Currency Exchange Systems

U.S. Patent No 9,830,580 (issued to nTrust Technology Solutions Corp. on November 28, 2017) relates to implementing a cryptocurrency mint. The network has a ring topology and includes computing devices that implement a plurality of nodes. The mint issues units of virtual currency to user accounts implemented by the nodes. Some of the nodes are configured to initiate (as a sender node) a transaction with a recipient node that transfers at least one unit of the virtual currency from a sender one of the user accounts to a recipient one of the user accounts. The recipient node validates the transaction, creates a receipt, performs an operation on the receipt to identify a storage node, and routes the receipt to the storage node. The storage node stores the receipt, identifies next storage nodes, and routes copies of the receipt to the next storage nodes for storage.

U.S. Patent No. 9,836,790 (issued to Bank of America Corporation on December 5, 2017) relates to exchanging a first currency for a cryptocurrency based on an optimal exchange rate and using a customer account and first and second float accounts of an exchange entity (such as a bank).

IoT/Sensor Information on the Blockchain

U.S. Patent No. 9,849,364 (issued to Bao Tran on December 26, 2017) relates to an IoT device having an accelerometer and storing sensor information from the accelerometer on a blockchain for tamper-proof storage of the sensor information.

Payment Processing/Transactions

U.S. Patent No. 9,818,092 (issued to Antti Pennanen on November 14, 2017) relates to processing cryptocurrency payments via a mobile device that incorporates use of a PIN to obtain private key information for validating a cryptocurrency payment transaction.

U.S. Patent No. 9,824,031 (issued to International Business Machines Corporation on November 21, 2017) relates to processing payments between an untrusted party and trusted parties, and recording the transactions using a blockchain.

Blockchain Integrity/Security

U.S. Patent No. 9,807,106 (issued to British Telecommunications Public Limited Company on October 31, 2017) relates to detecting and mitigating malicious blockchain transactions by determining whether incoming blockchain transactions deviate from a transaction creation profile.

U.S. Patent No. 9,785,369 (issued to Accenture Global Solutions Limited on October 10, 2017) relates to rewriting blocks in a blockchain to allow trusted parties to redact information from the blockchain, without causing the blockchain to fail for its intended purpose. For example, the parties may use a modified blockchain as if it was the earlier, and unmodified, blockchain.

Electronic Trading Settlement

U.S. Patent No. 9,794,074 (issued to Nasdaq Technology AB on October 17, 2017) relates to storing trades and/or positions that may be aggregated based on match messages from the various blockchain transactions that are recorded to the blockchain.

Electronic Ticketing for Venue Access

U.S. Patent No. 9,792,742 (issued to Live Nation Entertainment, Inc. on October 17, 2017) relates to using bitcoin and blockchain mechanisms to store and provide electronic tickets for access control (e.g., for physical turnstiles and other venue entry points) for venue access.

Supply Chain Management

U.S. Patent No. 9,641,338 (issued to SkuChain, Inc. on May 2, 2017) relates to using a cryptographic representation of value for goods in production and products at various stages through a supply chain.

U.S. Patent No. 9,641,342 (issued to SkuChain, Inc. on May 2, 2017) relates to tracking a chain of custody of an item in a supply chain using a distributed consensus network to verify one or more waiting transaction records for addition into one or more blocks in a block chain representing a cryptographically verifiable ledger.

Common Patent Misperceptions

Even when developers believe they have a potentially patentable invention, they often choose not to pursue patent protection due to one or more of a number of common misconceptions. Some of these misconceptions include the following:

Misconception: It takes too long to get a patent/the cryptocurrency and blockchain technology will be obsolete by the time it issues.
The truth is that it can take 1-3 years or more to obtain a patent. It is also true that a particular cryptocurrency and blockchain technology may evolve or become obsolete in that time. However, the misconception here is that this means the patent is necessarily worthless by the time it is granted. Many cryptocurrency and blockchain technology-related patents, if drafted properly, will not be limited to covering a single cryptocurrency and blockchain technology. If one carefully chooses the patents to pursue, and covers fundamental functionality or features that become standard features of cryptocurrency and blockchain technology or a genre of cryptocurrency and blockchain technology, the patent can have significant value for quite some time. Additionally, the U.S. Patent and Trademark Office has a method to fast-track patents. With this process, it is possible to get patents in less than a year.

Misconception: We are leveraging open source technology so it's not patentable.
There is no prohibition on patenting inventions that use open source (such as the bitcoin blockchain). The patentability results from the new features or functions you create using the existing technology.

Misconception: Most patents are invalid so why bother to pursue them.
It is true that some patents that issue are later invalidated, but that is more a function of the quality of a patent then an indictment on patents in general. With careful research, by using a patent attorney knowledgeable of the industry and quality patent drafting, many invalidity challenges can be avoided. If you pursue patents, do them right. Cheaply done patents, if invalidated, are worthless.

Misconception: Patents are too expensive.
The notion of "too expensive" is a relative matter. Patents can cost $20,000-30,000 or more to obtain. Given the millions to billions of dollars successful cryptocurrency and blockchain technologies can generate, are they too expensive? A properly crafted patent can deter or prevent copying of innovative cryptocurrency and blockchain technology features and avoid loss of hundreds of thousands or millions of dollars of revenue to clones. Additionally, patents for start-ups can also add significant value in other ways. More sophisticated cryptocurrency and blockchain technology investors understand the value of patents and this can help with funding. We have worked with many companies to license or sell patents that have generated millions of dollars in revenue for investments in the tens of thousands of dollars. These 10x or more returns provide great value and provide an example of how patents are not too expensive. Additionally, when cryptocurrency and blockchain technologies or cryptocurrency and blockchain technology companies are sold, patents can substantially enhance the value on exit. The bottom line is that like other business tools, there is a cost to obtaining a patent. But in many cases the cost can be a very sound investment.

Misconception: We would never sue so why get a patent?
Filing a lawsuit for infringement, or aggressively seeking licenses from others are examples of two of the "offensive" uses of patents. Patents also have "defensive" value that is often overlooked. For example, having a patent portfolio is a key deterrent in keeping others from asserting their patents against you. A competitor is much less likely to bring an action for infringement if they know the potential target also owns patents that can be used to bring a counterclaim. As another example, patents and published applications are the primary source to which patent examiners look during examination. If you do not file a patent application for your invention, it is possible that someone else may. If they obtain a patent this may require you to deal with their patent at a much greater cost than if you had filed and blocked them in the first place. Even if a later-filed patent is invalid, proving its invalidity may nonetheless create a cost in time and effort that could have been avoided.

Misconception: Even if we wanted to sue, we couldn't afford it.
This may have been the case years ago (if ever), but not so today. Now more than ever, there are a wide range of options for funding meritorious patent suits. More law firms will consider taking cases on a contingent fee basis. Additionally, there are a number of private equity firms that have created funds to invest in patent-centric businesses or even pure patent plays. If you have a valuable patent, there will be a way to fund the enforcement.

Misconception: I have not invented any new technology, I am just using existing tools/components.
One need not develop a whole new technology to have a patentable invention. In fact, most patents are merely improvements over existing inventions. More importantly, there is nothing that prevents one from obtaining patents on things that leverage existing tools/components. A concrete example from the old days of analog circuits may help. All analog circuits are a combination of existing components (resistors, capacitors, inductors, etc.). Yet, there are tens or hundreds of thousands of patents for circuits. These patents cover not the components themselves, but the unique combination of components and the resulting functionality of the circuit.

These are just some of the many misconceptions that we commonly hear. Many others exist.

How to Develop an Patent Protection Strategy

Two of the most important things that a developer can do to maximize IP protection for their cryptocurrency and blockchain technologies are:

- Be informed of the true facts regarding patents and not fall prey to misconceptions or "advice" from people who are not true cryptocurrency and blockchain patent experts.

- Consult with a patent attorney who specializes in patent protection for cryptocurrency and blockchain technologies. Even within the patent field, there are many nuances to protecting inventions in different industries. For example, patents for cryptocurrency and blockchain technologies require expertise in the areas of software, internet, business methods and knowledge of the cryptocurrency and blockchain technology industry, ERC-20 tokens, smart contracts and much more. Consulting an patent attorney who does not focus in these areas can lead to missed opportunities.

- We recommend that once you select a knowledgeable attorney, you sit down with the attorney and walk through all the details of your cryptocurrency and blockchain technology, your white paper, business model and product road map. Based on this, a competent attorney can help you develop a comprehensive patent protection strategy. Many attorneys will do such an initial meeting on a complimentary basis. If so, there is little to lose in participating in such a meeting and everything to lose by not doing so.

Conclusion

Many misperceptions cause developers to miss great opportunities to secure patent protection for their ideas. In part, this is due to a lack of a true understanding of what is protectable and/or not working with an attorney with the relevant expertise. Many cryptocurrency and blockchain technologies can be patented and many clones already are arising. Why make it unnecessarily easy for others to free ride on your hard work and creative genius?

About Sheppard Mullin

Sheppard Mullin is a full service Global 100 firm with 800 attorneys in 15 offices located in the United States, Europe, and Asia. Since 1927, companies have turned to Sheppard Mullin to handle corporate and technology matters, high stakes litigation and complex financial transactions. In the U.S., the firm's clients include more than half of the Fortune 100. For more information, please visit www.sheppardmullin.com.

Sheppard Mullin has a Blockchain Technology and Digital Currency industry team of over 20 attorneys with a broad range of legal backgrounds. For more information on the team, please visit our web page.

For further details on patents, please contact:

James G. Gatto
Co-Leader, Blockchain Technology and Digital Currency Team
202.747.1945
jgatto@sheppardmullin.com