Patenting Bitcoin

by François Veltz - Algopatent

10 June 2019

Blockchains are here to stay. Built on top of blockchains, crypto-currencies such as Bitcoin or Ethereum may have different if not divergent fates. A series of four articles investigate the matter of patents and blockchains, also known as crypto-ledgers. Blockchain-implemented inventions require good mathematical knowledge (e.g. cryptography, graph theory), coupled with sound economic vision (e.g. theory of the firm, incentives, etc), some game theory understanding (e.g. Prisoner's dilemma, cooperation, competition), in addition to solid computer science skills (e.g. software development, implementation and hardware infrastructure).

The first article attempts to provide, in plain English, technical definitions of blockchains and associated objects or methods (e.g. private versus public blockchains, proof-of-work, smart contracts, etc). The second article discusses patentability matters (e.g. from an EP and a US perspective, laws and Case Law are reviewed, examples of inventions are mentioned). The third article presents currently observed patenting activities (e.g. assignees, subject-matters and recent evolutions). The fourth and last article discusses prospective and horizons (e.g. opportunities and threats, vertical applications, IP scouting, etc). Patent drafting recommendations are proposed thorough the articles. Although interrelated, readers may jump directly to one article of interest.

The first section goes back to basics, from the technical perspective. The article attempts to explain in simple yet accurate words what is a blockchain, a smart contract and other related objects or components. Variants of these objects are discussed, with patent drafting in mind. The technical problems solved by these objects or combinations of objects are tentatively described. Blockchains are often associated with disruptive business models, where cooperation and competition can coexist, according to subtle nuances. Understanding the underlying technical and/or business incentives are certainly keys to build appropriate architectures. The article shows that intellectual genealogy of blockchains has ancient roots in distributed computing science, even if some of the latest developments can call for advanced mathematical and physics, including quantum physics.

The second section details current and foreseeable patentability issues. Being computer implemented inventions, blockchains present known (and generally mastered) patentability aspects (e.g. discoverability of cryptographic mechanisms, presence of open source code along closed code, forks, etc) but stress out particular points such as divided infringement, which shall be carefully considered due to the by-design distributed nature of crypto ledgers. The use of private and or public crypto-ledgers, along existing contractual framework agreements, tensions and evolutions between centralized (e.g. one or more nodes to gather data and/or handle processing), decentralized and distributed mechanisms (no central nodes, network of peers) can modify patentability opportunities and ways of drafting claims and specifications.

The third section does some data crunching in published patent applications, as of mid-2019. The article studies the general patenting landscape in terms of assignees and subject-matter. The numbers for now show a major presence of Information Technology companies (e.g. IBM, Amazon), while the expected presence of the finance industry remains significantly at lower levels (e.g. Goldman Sachs, VISA, etc). Chinese Universities have filed numerous patent applications in recent years. The filings of companies such as nChain can be analyzed.

The fourth section discusses patenting opportunities and threats. While core mechanisms (such as distributed consensus mechanisms) appear to have been largely patented or disclosed, there seems to remain numerous sweet spots. In the first place, vertical applications of blockchains do present many opportunities, because pioneer (if not essential) patents for now do not address specificities of technical domains (e.g. avionics, medical devices, privacy management, autonomous cars, GNSS, etc). The article tentatively proposes a systematic review of possible sweet spots, considering scales in space, time and other parameters. Last but not least, some aspects of the armament race with patents around the crypto currency Bitcoin are described.

As an ephemeral conclusion, blockchains and smart contracts are likely to have a sustained future, also with respect to patents. Solving very specific technical problems, blockchains are likely to be found in wide range of industries. If not solving core technical problems, as a transversal technical pattern, it may be applied to a wide range of inventions (involving a plurality of objects and presenting a trust issue at some places, e.g. security, reliability, etc). Concretely, this can translate into describing “blockchain embodiments” in specifications and may justify some dependent claims.

To protect your intellectual property, contact algopatent.com

I. Blockchains, Proof-of-Work validation systems and Smart Contracts (1/4)

Some recommendations for the drafting of patent applications relating to inventions involving blockchains or smart contracts.

1. Blockchains

A blockchain is a database that is distributed and secured by cryptographic techniques.

Transactions exchanged are grouped securely into "blocks", at regular time intervals and by way of cryptography, and thus form a chain. The different transactions recorded are grouped into blocks. After having registered the recent transactions, a new block is generated and analyzed. If a block is valid (as determined by the distributed consensus), this block can be time-stamped and added to the blockchain. Each block is then linked to the previous one by a hash value (checksum). Once added to the blockchain, a block can no longer be modified or deleted. This guarantees the security and immutability of the network of blocks. The chaining uses hash functions and Merkle trees. A hash tree is a set of interdependent hash value. The checksums are concatenated according to a tree structure. A hash tree allows verifying the integrity of a data set without necessarily having all of the data at the time of verification. The records in a blockchain are thus protected from forgery and modification by storage nodes: forging a block requires forging the entire chain, which makes the total cost of forgery prohibitive and ensures a level of confidence in the non-forgery of the blockchain as a whole. The transactions are visible throughout the entire network (except in the case of pruning).

To modify a blockchain, it is necessary (and sufficient) of take control of more of 50% of the nodes composing the blockchain. This is in practice very difficult to do (but not impossible, even for large public blockchains; in fine it is a matter of financial power and logistics).

It is worth noting that time plays an important role in blockchains (e.g. notions of broadcasting, propagation, latency, percolation in IoT, etc.) The distributed consensus implemented in blockchains is an answer to the "*Byzantine Generals' Problem*", wherein participants in an open network must agree on a concerted strategy to avoid system failure, while some of the participants can be unreliable, malicious or compromised. The distributed consensus of all network nodes may take a variable length of time depending on the technologies used. It can be accelerated using various techniques, notably "*sidechains*", which also increase the storage capacities.

Miners or mining nodes are entities tasked with supplying the network with computing power, to allow for the updating of the decentralized database. These miners can be paid through the distribution of cryptographic tokens ("*tokens*"). Other modes of compensation (additionally or by substitution) provide for commissions on the transactions.

A blockchain may be public or private, or take any intermediate form of governance, which may use different barriers to entry (Proof-of-Work validation systems). A "public" blockchain works *without* a trusted third party (model known as "*trustless*" or

"computational"), in contrast with a "trusted" model (centralized or institutional e.g. ECB, Federal Reserve, FDA, Patent Office, etc). A public blockchain does not generally define any other rule than that of the code established by the protocol technology and the software composing it. A "private" blockchain includes participating nodes in the consensus, which are defined in advance and then authenticated. Its rules of operation may be extrinsic.

2. Proof-of-work

To prevent or eliminate email spam, it had been proposed to associate a minimal price with the fact of sending one single email. This way, spammers sending millions of emails would have been quickly ruined. Proof-of-Work validation runs the same way: it is a barrier at entry.

In the distributed consensus framework, to respond to the technical problem of control of admission in a distributed system, it is possible to use validation by Proof-of-Work. From the mathematical point of view, a Proof-of-Work is "*difficult to provide but easy to validate*". Proof-of-Work validation systems are generally asymmetrical: the calculation which is required in exchange for a service request is costly for the requester but remains easily verifiable by a third party.

In the case of Bitcoin, an extremely difficult Proof-of-Work has been selected (*Hashcash*). This type of proof-of-work literally burns energy. When the planet is at war for oil, such a mechanism might appear pretty ugly (in terms of communication, because to secure transactions is "useful" per se).

In order to avoid what some consider as an ecological disaster, numerous alternatives have been proposed, or are currently under development. According to these alternatives, computations generally aim at being "useful" for the society, for example for medical purposes (e.g. research on cancer). Papers in economics would nevertheless argue that "utility" remains a relative concept (no universally useful computations do exist).

A major alternative to *Hashcash* is an approach called "*Proof-of-Stake*". In Proof-of-Stake systems, the creator of the next block is selected according to various criteria (e.g. random selection, wealth, age or the like i.e. the stake). Hybrid schemes also can be used. For example "Proof of Activity" can combine Proof-of-Work and Proof-of-Stake (e.g. Proof-of-Stake as an extension dependent on the Proof-of-Work timestamping).

From a patenting perspective, it may remain interesting to study alternatives to Proof-of-Work systems (e.g. "client-puzzle" patent US7197639), and to *Hashcash* in particular. From the mathematical standpoint, it is not clear how to configure types of computations tasks that cannot be optimized or otherwise bypassed. No immediate literature has been found on alternatives to Proof-of-work systems (as currently understood, the requirements of proof-of-work system are i) solutions are easily verifiable ii) difficulty for finding a solution is controllable. Many say that no "efficient" (relative concept) alternatives exist, or worse can exist. Even so, obtaining patents

provides control, either to encourage or discourage substitution. Public opinions also matter and would social choices be made, for example incorporating alternate forms of utility, such alternatives may end up to be incorporated in core protocols.

3. Smart contracts

Blockchains are or can become *programmable* through the use of "smart contracts". The field of smart contracts is emerging, complex and rich.

A smart contract comprises data and executable code.

As of today, smart contracts are short scripts which can be included in some specific blockchains (e.g. Ethereum). In the future, as envisioned by industry players, it may well be that entire full or complex programs can be stored and/or executed on blockchains. Complexity of smart contracts may increase "bottom-up", by complexifying smart contracts implemented in blockchains. Complexity of smart contracts also may increase “top down”, by engraving existing complex programs in blockchains.

3.1. Example of a smart contract

A simple example of a smart contract is a service agreement between two people. For example, let’s consider a party A which wishes to pay a party B for the performance of a service. The agreement is formalized by the creation of a smart contract in a blockchain. During the formalization of this contract, A pledges on the blockchain the amount of the remuneration intended for B. Once the service has been carried out, one of the parties can trigger the completion of the execution of the contract. It is automatically checked that the service has been carried out (manually by A, or by the intervention of an independent and previously authorized third party, or even in an automated way through the use of software). If the service has been carried out indeed, B receives the intended remuneration. If it has not been carried out, A recovers the amount of its pledge.

Noticeably, smart contracts can be created and concluded between machines.

3.2. Definitions

A smart contract (or *smart property*) is a software or computer protocol which facilitates, verifies and executes the negotiation or execution of a contract (such as payment terms, conditions, confidentiality, and even enforcement). A smart contract includes a software code that is stored and is executed on/by a blockchain and is triggered by external data allowing it to modify other data.

The expression "smart contract" thus refers to a set of computer protocols that emulate the logic of classic contractual clauses. A smart contract aims to emulate, or come close to, the logic of contractual clauses (contract law). Smart contracts are not strictly equivalent to contractual agreements. They make the violation of an agreement more expensive because they control an asset through digital means. A smart contract may not only define the rules and penalties around an agreement in the same way as a

traditional contract does, but it may also automatically enforce those obligations. It does this by taking in information as input, assigning a value to that input through the rules set out in the contract, and executing the actions required by those contractual clauses. Execution triggering conditions can comprise facts (information or inputs e.g. temperature, meteorological data, price of an asset, an event, etc) and/or logical rules (e.g. temporal rules such as expiry of delays, etc). Conditions may be internal and/or external to a given blockchain (e.g. a sidechain).

In some embodiments, the verification of the execution of clauses can be performed by humans (e.g. a named trusted third party) and/or machines. *Oracle* machines can be used. An *Oracle* as a mechanism for determining whether a test has passed or failed and is generally operated separately from the system under test. An Oracle can use one or more of heuristics, statistical characteristics, similarity comparisons, or can be model-based. Voting mechanisms can be used.

3.3. Specific features

By contrast with standard software, a smart contract is *stored and executed on a blockchain*. It thus inherits properties thereof, for example:

i) *immutability* of the corresponding code (given the high replication of chained blocks, it is may remain possible to corrupt one or more nodes but not as a whole for the entire blockchain);

ii) *auditability* of code (code instructions may be readable by man and/or machine in some situations; but transparency/opacity can be fine-tuned with encryption and obfuscation etc);

iii) *guaranteed and reliable execution* by/on the blockchain (even if many nodes are down or attacked, the program will be executed and distributed consensus will operate as well: the result of the execution will remain uncompromised);

iv) *automated* execution (triggering conditions may be met, as determined by machines, human intervention may not be necessary);

It also comprises properties that have to be carefully considered: code of smart contract, unless anticipated, may not be modifiable.

3.4. Common features with conventional software code

As for any program or computer code, different programming languages may potentially be used, with different expressivity and security models. An example of programming language is "Solidity".

The logic governing the enforcement of contracts can in fact be diverse. Along classical logic (for transactions between humans), other types of logic may be implemented (for machine-to-machine transactions, e.g. *fuzzy logic, or intuitionist, combinatorics, modal, propositional, partial, paraconsistent,* etc).

It is reminded that a software program, thus a smart contract, can be implemented in different ways. Smart contracts may take various forms (e.g. web services, agents, snippets, scripts, SOAs, APIs, add-ons, plug-ins, extensions, etc). A Smart contract may use using local and/or remotely accessed resources (processing, storage). It can be distributed, it can use or offer control or service APIs, it can use web services, it can be implemented entirely, or in part, as hardware embodiment (e.g. FPGA circuit placed in a smartphone).

Smart contracts, as computer software programs can be associated with various *regulation* mechanisms. Smart contracts can be independent or can be interdependent (chained, or otherwise linked). Smart contracts can be cooperative or not, competitive or not, convergent or divergent, synchronized or desynchronized, secured or not, formally proved or not, congruent or not, etc. Some programs may rule other programs (e.g. framework contract). Cascades of regulations may be implemented. Logical control layers may be articulated (top-down and/or bottom-up): from the control layers being very close to the data (e.g. programs manipulating data at dataset level) up to the objectives pursued by the service provider or operator in turn controlling smart contracts governing data processing.

As any other software program, a smart program can be linked to or associated with parts in *open source* and/or in closed source (e.g. while most of the code can be audited, some sensitive or security critical parts of the code may be in binary form, optionally obfuscated if not hardened). In an open source code, bugs or security flaws can be visible to all, but may not be quickly fixed. A smart contract may be open source in its entirety, but also can comprise some parts in binary code (the source code being not easily obtainable by reverse engineering, i.e. security by obscurity), thereby combining the "best of both worlds" (auditability and trust for some parts, proprietary control for other parts of the code).

As any program or code, smart contracts may present a substantial surface for attacks. Smart contracts need to be "secure" from a computer security perspective. It may possible to develop entirely new programming languages for encoding smart contracts. An example of programming language is "Solidity". A program or smart contract may be secured or may use various *encryption* schemes (including but not limited to post-quantum cryptography, quantum-safe cryptography, Quantum-Key-Distribution, etc). In addition to the code of the program being open source and/or closed source, code escrow mechanisms can be used (i.e. combined with restricted access, under (automatable) conditions and/or by a human organization). Many countermeasures may be taken (e.g. polymorphic code, honeypot, etc).

Regarding form, a program or smart contract may be human and/or machine readable. By construction, an (executable) program is machine-readable: facts and rules can be manipulated by machines. Machine readable instructions cannot be read by humans. Human-readable rules or programs generally (often but not always) can be read by machines (e.g. some natural language ambiguities in practice cannot be handled by machines, now or in the foreseeable future). Depending on applications, it may be advantageous that rules coded in the program can be read by humans (for transparency, governance, control, etc). In some cases, the program may be written in executable pseudo-code, readable both by humans and by machines. In other

situations, machine-readable code may be transcoded or otherwise visualized in human-understandable form (e.g. human-readable icons).

3.5. Validity and perspectives

Smart contracts potentially can find a wide range of vertical applications, in different technical domains. Naturally, at first, they may find application in financial instruments such as bonds, shares and their derivatives, contracts for insurance and many other financial areas (the age of programmable "*money*").

To our knowledge, the validity of smart contracts is yet largely to be assessed and confirmed. For example, there are questions about the electronic signature. Electronic signature laws generally require the electronic contract signature to be "attached to or *logically* associated" with the contract terms. There are currently passionate debates in the Bitcoin community about a data pruning technique called "segregated witness", consisting in separating signature data (witness) from the transaction data. While the objective of such a data pruning technique is to increase the size of a block (which is highly replicated in the distributed network), to get a supposedly better use of it, it may be possible that this technique proves to be harmful - if not incompatible - with Contract Law ("blockchain evidence"). Opponents to the "segregated witness" option declare that the network would become less reliable. Criteria such as "reproducible content", "link of the signature to the record during transmission and storage", "signature contain in and attached to" and others may be endangered by such data pruning techniques. Would some specialized nodes keep signature data, these nodes would be become "trusted" or privileged nodes (thus bottlenecks, at worse "government-authorized validators"), which can be antithetical with the decentralized trustless Bitcoin system. What such data represents in quantitative terms remains unclear, as signing parties can be keep their own copies (and the volume may well stay perfectly manageable). How exactly "contract terms" can be stored also seems questionable or to be investigated (e.g. link to human readable forms, etc).

With respect to developments and horizons of smart contracts, computer security and networks of smart contracts can be considered. Chains or networks of contracts in particular can be tested (e.g. simulated, emulated, etc). The property of auditability can thus increase trust in the program articulating data collections. Automated enforcement of the smart contract enables larger automations schemes, and in particular allows controlling data flows of data. Built-in financial features enable many further developments, such as micro-payments (if not nano transactions in the world of Internet of Things) and revenue sharing tied with access to data (monetization). Considering networks of smart contracts, computer security considerations become increasingly complex (e.g. systemic risks).

4. Bitcoin and crypto-currencies, built on top of blockchains

Bitcoin is about money. Money rules the world. A fascinating fight, on the legal side, may surge along the technological race. Bitcoin and other crypto-currencies combine different technological bricks, comprising one or several blockchains, Proof-of-Work

validation systems, different cryptographic signatures, etc. Crypto-currency is created and allocated to miners as payment for the processing of transactions in blockchains.

4.1. Bitcoin, using blockchains

The history of Bitcoin is now well documented. Interested readers can refer to the *Wikipedia* pages (in English), the founding document published in 2008 by *Satoshi Nakamoto* entitled "*Bitcoin: A Peer-to-Peer Electronic Cash System*", the various posts of Satoshi Nakamoto ("*The Book of Satoshi: the Collected Writings of Bitcoin Creator*") and the articles of *Andrew O'Hagan* ("*the Satoshi Affair*"). The books of *Tapscott* and *Antonopoulos* can also be recommended.

Bitcoin was conceptualized before the year 2000 and is officially born in 2008. It made ripples in 2011 (review in *Wired*) before becoming mainstream in 2013, and is now claimed by the Fintech industry. The crypto-currency caused palpable industrial and financial shockwaves (e.g. mining activities, real transactions, involvement of financial regulators, etc.).

Bitcoin is a libertarian political project at start, according to an underlying economic vision (inspired by liberal thinking). It targets "cryptographic cash" (within the monetary meaning), i.e. a currency without an institutional regulator (thus without the possibility of state intervention) but according to an objective and non-manipulatable (or difficult-to-manipulate) computer model, with guarantees in terms of privacy and liquidity. Bitcoin is meant to be secure mathematical *cash*, rare, without any institutional control ("*real hard money*"). More profoundly, Bitcoin aims to replace the "*credit-based economy*" with the "*equity-based economy*", which leads to radically different horizons in terms of business models (and which are generally patentable). The debates are well fed as to the legal and fiscal status of this new subject (e.g. unit or account or commodity rather than currency) and its regulation (i.e. taxation)

From a technical point of view (keeping in mind the question of intellectual property rights associated with Bitcoin and blockchains), one shall not forget that Bitcoin is based on cryptographic foundations that are well controlled, but continues to evolve. Technically, Bitcoin integrates proven and old computer technologies. The intellectual genealogy of Bitcoin is known (B-money of Wei Dai 1999, Nick Szabo 2005) probably even further back, to cyberpunk and cypherpunk circles (1980s).

In 2019, Bitcoin is at a historical turning point. Today Bitcoin represents an infinitesimal fraction of global monetary exchanges and the number of transactions per second is still very low. The community actively seeks scaling ("*Bitcoin needs to scale*"), which feeds the passionate debates on the technical options to be taken, and has led to *forks* (splitting of Open Source projects) which were high-profile (Bitcoin Cash ABC versus Bitcoin Cash SV). Variants of Bitcoin, called "AltCoins" (e.g. *Litecoin, Namecoin, Swiftcoin, Primecoin, Blackcoin, Dash, Ethereum, Zcash*, etc.) are pursuing different compromises, in terms of their model (inflationary or deflatory), access, Proof-of-Work validation systems if any, types of cryptographic signatures, the use of *sidechains* or *off-chain* mechanisms, etc. For the proponents of Bitcoin, these variants are often perceived as harmful (abandonment of sovereignty, loss of

freedoms, energy wastage in terms of software development efforts, hardware resources lost in terms of network, etc.).

4.2. Patents on Bitcoin

Numerous patent filings refer to "Bitcoin" in specification, or even in claims. Some patent filings appear to be directly addressing crypto-currencies, others have large scope. The portfolio of the nChain company is studied hereinafter (as of 2018).

The technologies that form the basis for Bitcoin, and in turn for "AltCoins" (cryptographic currency alternatives to Bitcoin), are for the most part distributed computing techniques, which have long been of interest in many industrial areas (Internet, telecommunications, scientific computing, robotics, industrial automation, etc.). For example, the distributed consensus problem is a known problem in distributed computing theory, which dates back to the 1970s (e.g. IBM patents).

Currently, all technology components used for crypto-currencies are likely to be sophisticated further and therefore to result in patent applications being filed. As a recent example, *Boneh-Lynn-Schacham* signatures have been considered in place of *Schnorr* or elliptic ECDSA signatures. Proof-of-Work validation methods are also likely to evolve rapidly.

Regarding the specific case of Bitcoin and its declinations (e.g. Bitcoin Cash, or its forks ABC or SV), it has first mover advantage but it probably comprises several flaws (e.g. no built-in governance, limiting factors for scalability, etc). Bitcoin has funded hostile forces against it, but also supportive crowds. In our opinion, an important question lies in the possible rat race between finance and information technology. Finance operators such as banks and finance giants such as Goldman Sachs may build new IP portfolios, but these take years to build. For now, players in finance have surprisingly low numbers of filings. By contrast, IBM and the major players in IT have way more patents that the Fintech can ever dream of. IBM alone has more than 120 000 published patent applications, in many different areas (from distributed consensus to fundamental cryptography). In between IT giants and finance giants, startups or other players may try to influence technological directions with patent filings. They probably have limited but reasonable chances, *a fortiori* with strategic alliances (e.g. Google, banks). If for example merchants (e.g. Amazon) would provide the desired hash power to scale the crypto-currency, and if concomitantly the use of the crypto quickly spreads, then Bitcoin might indeed become unstoppable. There is no doubt that top executives in IT and finance, not alone governments and central banks, are monitoring this closely. Patents may play a role. That’s a paradox, given the roots of Bitcoin (rejecting institutions). For sure, the legal battle will be epic.

II. Patentability of blockchain related inventions (2/4)

As *software* inventions, Bitcoin, crypto-currencies and blockchain related patent inventions are (in practice) generally patentable. Their technical character, inheriting of strong cryptographic flavor, is favorable to patentability. Yet some inventions may be qualified as *business methods* (administrative, economic practices, etc), which are generally barred from patentability. The frontier between software patents and business methods is porous: patent drafting know-how can make the difference (e.g. terminology and some adjustments brought to the invention if necessary). The following sections specifically consider patentability in Europe. Additional sections describe specificities in the USA.

The inventions currently published have interesting features, bordering on delicate matters regarding exceptions to patentability: (i) software patents (ii) mental acts and intellectual methods, (iii) business methods, (iv) representation of information. Each of the exceptions can lead to adjustments in language. The following sections review the specific case of blockchains relative to the criteria commonly considered for each type of exemption from patentability.

1. Computer-implemented inventions

Blockchain-implemented inventions pose the conventional problems that are now posed by the majority of inventions implemented by computer but aggravate them somewhat through the use of blockchains as distributed databases and encrypted content.

Counterfeiting may occur at different places:

- blockchain-implemented inventions may comprise one or more known blockchains, along a plurality of other objects, exterior to the blockchains: these inventions if claimed may be reproduced;

- within blockchains, smart contracts for now are short scripts, but they are likely to evolve into complex programs, highly replicated across the distributed database. These complex programs may implement patentable and/or patented inventions;

- blockchains *per se*, theoretically, may be claimed (as combinations of known or unknown technology bricks, e.g. validation systems, signature schemes, pruning techniques, tiered architectures, etc). New types of blockchains are regularly popping out on the market (nano transactions for M2M, etc).

The following sections discuss specific traits of blockchain-related inventions: i) discoverability and ii) divided infringement.

1.1. Discoverability

A major legal aspect for computer-implemented inventions lies in the discoverability of these inventions. This discoverability can evolve over time (via the software product itself, its form e.g. *Open Source*, and its documentation). At any given moment, it may

be immediate or may require reverse engineering. Discoverability is not appreciated by patent examiners, but it is a critical factor in the understanding of counterfeiting (e.g. counterfeit seizures and the interpretation by judges and/or juries). Discoverability also mirrors the readability of inventions for opposing third parties, e.g. industrial property attorneys conducting freedom-to-operate opinions.

Like any invention of a software nature, the discoverability of inventions using blockchains is to be judged carefully. Blockchain-related inventions are generally characterized by a rather low discoverability. The data centers are almost never public and in general they are very difficult to access (e.g. necessity of counterfeit seizure operations, injunctions, etc.). In addition, the intensive use of cryptography undermines the discoverability of inventions. In addition, data in blockchains can be stored in clear text, but also in cipher text. Encryption techniques, used by default i.e. by design in blockchain related inventions, can significantly harden the detection of infringement.

The portfolios (*wallets*) include graphical interfaces, whose *frontends* are detectable (and of value from the point of view of their discoverability), but they represent a very small part of the technology, which runs mainly on the *backend* ("*patents buried deep in data centers*"). By design, blockchains, or part of them, are replicated in many nodes of the network, but this data may remain little informative. The hash value processing software can be implemented locally (accessible) but also in reserved places in the network (e.g. inaccessible caches).

With regard to Cloud computing inventions, patent attorneys also can take care to envision and write down "open loops" (i.e. interactions with the intervention of the user, therefore visible and detectable steps) but also the automation - in the long term - of these feedback loops (i.e. according to closed loops, giving the quantitative criteria allowing logical decision-making by the machine). Man-machine interactions are also at the heart of “explainable A.I.” that is Artificial or Augmented Intelligence which can be acceptable to the regulators (no black-boxes with unpredictable behaviors).

1.2. Infringement

To date, there seems to be no patent litigation in the emerging field, aside code forks.

Historically, "Cloud computing" architectures have increased the relevance of "divided infringement". Divided infringement can also be referred to as "joint infringement" or "contributory infringement". Divided infringement designates a form of patent infringement liability which occurs when multiple actors are involved in carrying out the claimed infringement of a method patent, and no single accused infringer has performed all of the steps of the method. Mashups and other composite applications involving a plurality of servers have focused patent attorneys to draft patent claims directed towards the main provider of a service, or that can be read on multiple entities.

To these existing difficulties, blockchains seem to raise new and entirely different legal problems.

A salient trait of blockchain-related inventions stems from the *distributed nature* of blockchains. As many parties are involved, by design, it may become very easy to

detect possible counterfeiting: by seizing one single node replicating all data and/or programs embedded in the blockchain. At the same time, it may become very difficult to catch a myriad of counterfeiters, as the database is highly replicated.

In other words: if each node of the network has got the same copy of data and programs, it is necessary and sufficient to get hands on one single node to assess counterfeiting. But even if proven, what can one do against thousands of counterfeiters?

Another factor lies in code size. As of today, smart contracts are short scripts and it is unlikely that these scripts can implement patented inventions. But in the future, complex programs i.e. significant software codes may implement a plurality of invention (e.g. Internet of Things, self-regulation of autonomous cars, etc).

Some factors can temper previous assessments. There are generally some *tensions between centralization, decentralization and distribution* mechanisms. Centralization and decentralization refer to the fact of having more or less "centers" in a given architecture. Distribution designates systems which are theoretically corresponding to peer-to-peer systems, each node being equals, i.e. with no privileged nodes. In reality and in practice, pure distributed systems are rare; due to technical and/or business compromises, some nodes can have particular roles (e.g. indexing, taxation, caching, etc), and following, data and processing steps may be assessed differently at some particular nodes, with some nodes having more liabilities than others. For example, in private blockchains, the number of players may be fairly limited, and the infringement of a patent method may be determined. Gathering and owning "big data" (to perform added-value analytics thereon) is often at stakes: some parties can be fighting hard to have privileged roles. For example, in privacy management using blockchains, there can often remain an intermediary of choice, detaining ciphering keys. Also, exposing APIs can lead to disclosed patented method steps.

It remains that, combined with the (hard) discoverability of blockchain-implemented inventions, counterfeiting may become excessively hard to detect, and then to enforce. As with software patents, patent drafters shall attempt to draft claims ingenuously, i.e. in a party-centric perspective (e.g. what manifest method steps does part B perform in its interaction with A and C?). In addition, patent attorneys may focus on private blockchains, where the number of players is reduced. Smart contracts may end up conveying computer implemented inventions.

1.3. Open Source Software

Open-source code doesn’t necessarily restrict the ability to patent the underlying technology. The fact that some software be open-source does not necessarily means that implemented inventions therein will be discovered (it may be very difficult to assess a spaghetti code).

Depending on the case, it may be advisable to annotate - or not – a code available in open source. On the other hand, the code can be intentionally obfuscated, even hardened or shielded.

Regarding smart contracts, the open source character also refers to *readability* of these smart contracts (see previous article).

2. Mental act and intellectual methods

With marked mathematical flavor, the claims of some blockchain-related inventions may appear unfavorable, at least at first. One cannot patent pure mathematics. The use of a language with excessive mathematical character generally can raise objections of abstraction, or of mental acts.

Conversely, to succeed, a claim must overall use the most "technical" words possible (which is ultimately in line with social requirements). Experienced patent attorneys know from experience what are the effective compromises.

In the case of blockchain-related inventions, it may be recommended to underline - and if possible to develop - the aspects in relation to tangible systems or *specific hardware*. For example, one will not stick to general-purpose processors (*see infra*), but depending on the case, will highlight embodiments involving FPGA processors, distributed computations specific to the inventions, the use of *multi-core* or *many-core* processors for optimization purposes, etc. It may also be appropriate to underline aspects specific to the *automation* of tasks, for example in that they are not manually and/or cognitively feasible (e.g. methods of high frequency, real-time, volumetry and scales, etc.).

3. Business Methods

Blockchain-implemented inventions often present economic models which are emerging, or radically disrupting existing practices. These business models are generally reflected in the words that are used in claims, for example, words or expressions such as "*merchant*", "*commission*", "*peer-to-peer lending*", etc.

In Europe, plans, principles and methods involved in the exercise of intellectual activities, in gaming or in the field of economic activities, are considered "non-inventions" within the meaning of Article 52(2) and (3) EPC. Nevertheless, implementation by computer may render a commercial method patentable (if the improvement provided by the device is not only observed in the economic sector).

The terms imported from the areas of trade, business management and finance must be, to the maximum extent possible, defined in the most quantitative terms possible. If only definitions are possible (i.e. circumlocutions or paraphrases or definitions specifying what is heard or covered by a given word), it should be borne in mind that these definitions are likely to be introduced in the claims during prosecution: extreme care must be taken as to their formulation, in the same way that it is brought to the choice of words in the claims.

In Europe, and particularly in the last few years, the clarity of the claims under Article 84 EPC is becoming more and more imperative. For example, imprecise terms such as "*visibility*" in the expression "*visibility of a smart contract*" are likely to raise objections.

In practice, it is essentially a question of terminology, which must be chosen as technical as possible (if this is possible, not always the case). Vocabulary with economic connotations would be better replaced with vocabulary considered "technical".

Technical words such as "*message*", "*network*", "*node*", "*key*", "*party*" are widely accepted by patent examiners. If possible, it is preferable to avoid commercial or administrative language using words like "*merchant*", "*price*", or "*payment*". Such objects can be either abstracted into words such as "*entity*" or "*machine*" or "*server*" (because the quality of being a merchant is non-technical). At least in Europe, the minimal amounts of words specific to the target field should be used, at best. For example, the nouns "*share*" or "*payment*" presents a marked financial flavor; hence its use shall be minimized. Advantageously, such terms shall be replaced by appropriate synonyms. WorldNet and other dictionaries for example indicate the following synonyms for "share": *portion, part, percentage, capital stock portion, parcel, and contribution*. Some synonyms may be appropriate, or not. In some cases, there are no real alternatives. The expression "*smart contract*" is an embedding's which is relatively recent, with floating or fuzzy borderlines (despite Wikipedia pages, the terminology may be argued as non-stable). This expression can be instantiated into a "*program*" or a "*protocol*". Even if some words can be accepted *a priori*, it can be advised to stay away from the field of business. For example, transactional systems are generally patentable (tourism industry), but by safety the term "*transaction*" may be replaced by "messages passing" or the like, to underline the technical features lying underneath.

Beyond the choice of words i.e. the only choice of terminology (constitutive of the "flavor" of the claims), it may be recommended to insist on the *technical* characteristics of the invention and the *relationships* between the carefully chosen words.

The technical nature in particular may be strengthened by the use of carefully written definitions (these definitions in themselves constituting "second curtain" claims, in that they can lead to reshaping the claims as filed). Then, with regard to the relationships between words, a generally fruitful approach is to consider a plurality of objects being handled. For example, handling a plurality of smart contracts almost immediately raises exciting questions. The fact of having a plurality of economic actors can be translated technically by the implementation of "*multi-party computing*" or optimization mechanisms; *multi-objective optimization* for example. In general, as a claim can be represented by a graph (relationships between objects), one may consider the various modalities of interaction or regulation associated with the interacting objects (examples of questions: *Where are the control points of the system? Is the system controllable? What are the systemic risks, if any? What regulation or man/machine interface* do apply (e.g. automatic triggers, thresholds)

At the periphery of the invention, in order to reinforce the technical nature of certain inventions, it may be appropriate to consider variants of features or words in claims in a systematical way, in order to exhaust them and write them down in the description, as a "reservoir" for later claim shaping during prosecution. For example, for an invention dealing with computer security, one may consider further protection by

biometrics, security by encryption, using post-quantum cryptography, using of centralized or distributed database, etc.

Requirements for technical features of blockchain related inventions also can call for the study of many underlying aspects, including the types of logics implemented in smart contracts. Also, the modes of *"commissions",* "*fees*" or other *"incentives"* can be investigated. The handling of a plurality of objects can be investigated with respect to systemic effects, "cybernetic" regulation, learning, etc.

4. User interfaces and representation of information

With respect to interfaces and representation of information (which is non-patentable in most jurisdictions), the boundary is sometimes complex between substance and form. With sufficient know-how in the drafting of claims, the description and claims regarding the representation of information can be formulated in such a way that the patentability situation improves. European Case Law first evolved in 2012 and now considers more favorably the inventions that improve decision-making or reduce the cognitive load associated with the use of human-machine interfaces.

At times, the invention may even be developed, in substance, because of these reasons of a legal nature. For example, patent attorneys can try to *quantify* the representation of data as much as possible. For example, a "*symbology*" (collections of icons or symbols) and the display of these symbols can be assessed according a perspective of quantized graphical superposition (with predefined intermediate symbols). The triggering of actions (causes) and the logical rules managing the displaying (consequences) will be advantageously explored, developed, described and claimed. In general, it is useful to describe and claim the underlying logic governing the actions carried out by the machine, what are these actions, the way in which these actions fit into the wider process, etc. It is generally positive to emphasize the possible synergies between the logical interfaces and the physical systems (for example "*force touch*" systems may imply many subtleties in user commands, e.g. speed/pressure of a gesture by the pilot in a plane that indirectly indicates the state of mind e.g. panic, hurry, calm, etc of the pilot when entering data). These considerations may be adjacent to the very gist of the invention, but they frequently generally allow patentable and blocking positions for third parties.

Published patent applications often reveal claims requiring a user validation ("open-loop", for example requirement of the patient approval before an insulin injection). Within the meaning of European law, claims with such open loops (with human intervention) may be inappropriate; it is prudent to provide "closed loop" embodiments, along open ones and to describe the quantitative decision criteria for closing loops (machine decisions). Similar examples may be provided in aeronautics, wherein the pilot might the final word… or not (dronification of planes).

5. Consideration of additional regulations

To further complicate the situation, the technologies relating to blockchains or smart contracts often concern industrial sectors (e.g. medical, avionics, robotics, etc.) that are *already* enrolled in binding regulatory frameworks.

The applicable rules and standards structure their markets. Indirectly, existing regulations structure patent application claims (to be marketable, an invention must comply with the regulations in force). These rules, norms and standards (which are part of the state of the art) often result in concrete technical characteristics. The involvement of a third party regulator limits the realm of what is possible. If an invention is too different from formal requirements, it cannot be implemented and will remain speculative. If an invention is directly related to them, it will not be patentable in view of the state of the art.

For example, in the medical field, patented inventions must meet the rules by the FDA (*de facto* worldwide rules in globalized markets). The "artificial pancreas" (closed-loop system, that is without human intervention) is not yet authorized. In reality, "open loops" systems (with the patient feedback, e.g. confirmation of bolus injection) are patented; corresponding claims include user confirmation or moderation steps. Would closed-loop systems be suddenly authorized, most of pending or granted claims would be obsolete (would not read on medical devices). In such systems, it is wise to anticipate complete automation (different future of regulations). Likewise, the use of blockchains will raise many questions of a technical nature, but also of a regulatory nature.

In the field of aeronautics, avionics is structured by the FAA. The certification of aircraft imposes boundaries between avionics-type equipment ("closed" world) and non-avionics type equipment ("open" world). In practice, this distinction may be tentatively quantified, for example according to reliability criteria (for example) specified in patent claims. Avionics may make multiple uses of *blockchains* to supplement, or substitute in part, the existing models, which will have to comply with existing and foreseeable regulations. In other words, patent filings in this area will therefore have to become even more sophisticated.

In the field of banking, banks are increasingly using blockchain-related inventions or preparing for them - will soon have to comply with the GDPR directive, which is now heavily influential in Europe. Among other requirements, the "right to be forgotten", specific to the EU when compared to the USA, will require special - and transferable - handling of read-write rights in databases. Taking the investigation even further, it appears that *redactable* blockchains (modifiable subparts) will be needed, somehow in contradiction with the root principles of blockchains. Digging even further, quantum mechanics may be needed to get unclonable systems (anti-copy of fake or deprecated information).

In the field of autonomous cars, inventions regarding self-driving cars may involve privacy aspects, which may in turn invoke the use of blockchains and/or liability systems encoded in smart contracts.

In short, the consideration of regulatory requirements - present and future - must therefore be added to the technical and legal considerations, when dealing with blockchain-related inventions. The regulatory complexity may therefore directly impact the corresponding patent application claims. In the long term, it is possible that previously separate technical domains can join together (hybridization of technical domains).

6. Patentability in the USA

Some noticeable decisions by the Supreme Court shaped the US landscape regarding business methods and software patents.

In 1998, the decision "*State Street Bank & Trust Co v Signature Financial Group*" established that business methods could be patentable and led to a tsunami of computerized business methods. In 2014, the decision "*Alice Corp Pty Ltd v CLS Bank*" held that financial business methods implementing a "fundamental economic practice" were likely un-patentable abstract ideas, unless including "technological" advances.

To date and in practice, a test in three steps is applied, the third step being critical. It is first considered whether the invention (i.e. the claims) is directed a statutory category (e.g. a process or a system). This step rarely is blocking. Then it is considered whether the invention is directed towards to a judicial exception (an abstract idea), for example towards an invention which can be performed mentally (compare and/or organize data) or by man using pen and paper. Considering mathematical algorithms, it is generally the case. Then the third step considers whether the claims "amount to significantly more" than the abstract idea. Several sub-criteria can be leveraged. The use of a generic computer (e.g. Von Neumann architecture) or a simple display device is generally not sufficient to satisfy to the third step of the test ("high level of generality", "well-known interface", etc). Time passing by, requirements may even escalate. In some of our prosecuted cases, it even has been alleged that an MRI (magneto-resistance imaging) device is a "generic" device. Limitations to specific fields of use (for example medical applications, logistics) also may not be sufficient, even if the policy "risk" for the Patent Office to issue overly broad patent is significantly decreased. Purposes or the field of use limiting the scope of the claims may not give "life, meaning and vitality" to the claims. In order to amount to significantly more than an abstract idea, such limitations to specific fields of use have to be "meaningful", i.e. which have to present an intricate, intimate or otherwise deep relationship with the envisioned field ("confining the abstract idea into a particular useful application"). In practice again, one can see that accumulating limitations (tangible devices to perform the invention, specifying fields of use, synergetic effects) can lead to patentable subject-matter.

Blockchain patent applications may be considered software patents. An invention that improves the technological functioning or processes of a computer itself may be patent eligible. The US Case Law seems increasingly consistent with the European practice, putting emphasis on technical character and technical effects (not indirect economical effects).

7. Patentability in other jurisdictions

To our knowledge and experience, prosecution in China is very similar to the European practice. A patent application drafted for Europe may pass in the USA, but the opposite may not be true (due in particular to the lack of mentions of technical effects associated with claimed features).

For other jurisdictions (e.g. JP, KR, CA, AU, etc.), it is advisable to consult a national patent attorney.

III. Published patent applications of blockchain related inventions (3/4)

The last few years have seen increased patent filings in relation to the technological bricks of Bitcoin (e.g. blockchains, Proof-of-Work validation systems, cryptographic signatures, etc).

Blockchains are now reaching vertical applications (aeronautics, supply-chains, medical devices, after finance, insurances and banking, etc). Regarding crypto-currencies, different interest groups have formed, in correlation with increasing political, economic and financial stakes. Companies in the banking sector file patent applications (e.g. Bank of America, Visa). The finance giants (e.g. Goldman Sachs) take a stance and file as well. Companies in related sectors such as Amazon and IBM are specifying their filings. Venture capital are funding many start-ups that hard-code, and seek exclusive rights. The positions of the regulators, e.g. the Fed and ECB, are regularly adjusted. Some Nation States plan to create national crypto-currencies (e.g. crypto-Ruble or crypto-Yuan). Patent groups are coming to light (e.g. the "Blockchain Patent Sharing Alliance" in October 2017). Some other entities are discussing patent pledges (MIT, Coinbase). Some companies like nChain are making their main focus of patent filings and aim to influence the market (in favor of Bitcoin Cash and now its Satoshi Vision fork). In the first approach, it is somewhat paradoxical that the defenders of Bitcoin, which aims to exist independently of States, seek to obtain patent rights, which by nature are mechanisms of ownership imposed by Nation States. In reality, the need to reaching the general public involves compromises that seem to take place on many levels (governance, traceability and taxation, standardization, collisions, congruence's, compatibilities, etc.).

1. Fast facts

1.1. Number of published applications

Search tools in patent databases allow clearly showing the increase in filings, confirming intentions to control the sector.

Mot-clef	**In** *claims* **(number of published applications)**			**In** *description* **(including claims) (number of published applications)**		
	End 2017 (Nov.)	Mid 2018 (July)	Mid 2019 (June)	End 2017 (Nov.)	Mid 2018 (July)	Mid 2019 (June)
"**bitcoin**"	29	207	305	1527	2433	3768
"**blockchain**"	123	626	**1776**	512	1777	**4168**
"**smart contract**"	33	245	**1143**	226	764	**3303**

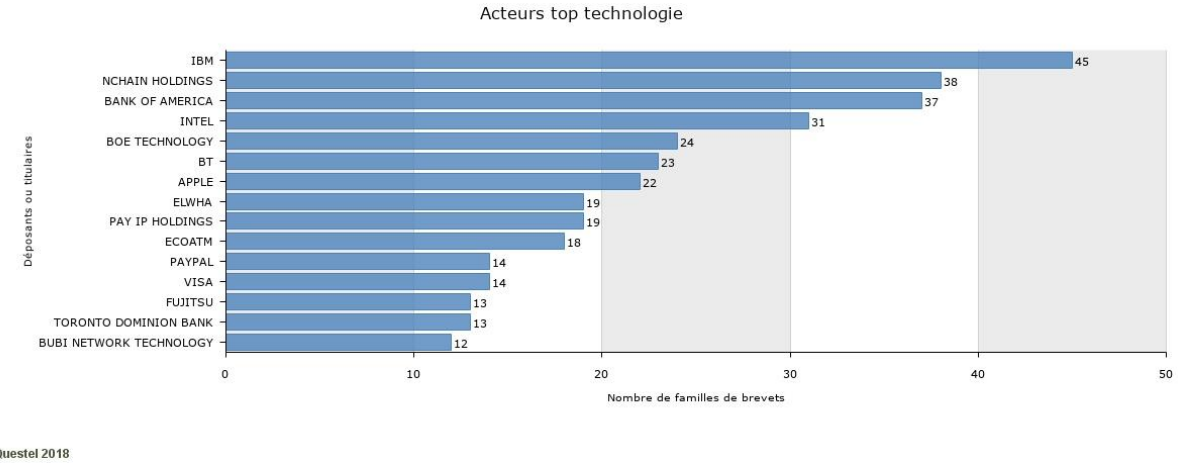
Source: Questel Orbit, retrieved November 2017 and June 2019 (covering 18 months)

The figures above, along search reports, seem to indicate that the terms "blockchain" and "smart contract" have massively entered the patent corpus, *and noticeably the claims' corpus* (over the last past year in particular). Bitcoin is not frequently used in claims, as expected, but is largely invoked in the specifications. Yet, even if the words

may appear clear for the skilled person (the Examiners), and even if definitions in Wikipedia appear relatively stable, it still can be recommended to carefully define these terms and to provide examples, as these techniques are associated with very specific properties (software executed in parallel for smart contracts, different types of blockchains, etc).

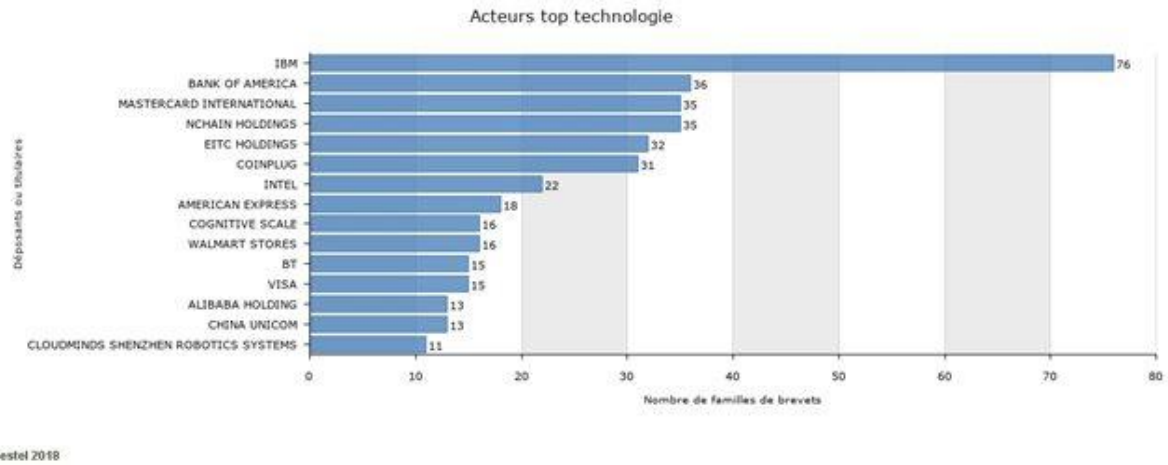
1.2. Assignees

Between November 2017 (the beginning of writing this article) and July 2018, a great number of filings were observed coming from Chinese universities (cumulatively exceeding 300 filings).



« bitcoin » anywhere in specification, number of families per assignee, Questel, July 2018

Other noticeable assignees comprise (selection): WALMART (11), MASTERCARD (10), NOKIA (10), UPS (10), ALIBABA (8), COINBASE (7), AMAZON (5), BITMAIN (10), NASDAQ (5), SAMSUNG (3), GOLDMAN SACHS (2), MICROSOFT (2), AMADEUS (1), ID QUANTIQUE (1)



« blockchain » anywhere in specification, number of families per assignee, Questel, July 2018

Blockchain-implemented applications typically fall within the class range IPC G06F (data processing), G06Q 30/00 (electronic commerce) and G06Q 40/00 (finance, taxation).

Patent applications published to date seem to be as much about the heart technology (e.g. "sidechains" which for some betray the founding idea), as it is about improvements, whether the latter are significant (for example programming blockchains) or accessory (opportunistic filings on the interfaces of "wallets"). A wealth of vertical applications can also be detected.

To date, it is now clear that the technical potential - and therefore of patenting - of this family of technologies is substantial. Firstly, the Fintech sector as such is in turmoil and continues to invent at a steady pace. Like a Precambrian evolutionary explosion, many of the core technologies used by Bitcoin are rapidly evolving.

For example, the substitution of the original "Proof-of-Work" algorithms (based on the notion of investment) by "Proof-of-Stake" algorithms leads to substantially different systems. Moreover, by transversal effect, many technical fields can reincorporate Bitcoin technology bricks, sometimes modifying them. Related or distant technical fields can quickly hybridize with core technology bricks (e.g. management of personal data, the Internet of Things, transactional systems, etc).

In the future, one can probably expect increasing cross-fertilization of technical domains. In the IT sector (Information Technology), the patent portfolios of IBM and GAFA account for a total of hundreds of thousands of applications and patents issued (the IBM portfolio alone is currently of the order of 50 000 titles). A fraction of these inventions is likely to be implemented by industry players. The reasoning in "silo" of Patent Offices should allow, for some time, to file patentable transpositions (applications of blockchains in the travel industry, in healthcare, and avionics industries, etc.).

2. Examples of inventions

The following examples show only a fraction of the great diversity of topics covered in published applications to date.

First example: instead of advertisements displayed on web pages (often considered as intrusive), in exchange for access to desired content, it is envisioned to locally execute software code in the client web browser to mine crypto-currencies, in order to remunerate the creator of the visited contents. In fact, these mechanisms are already implemented and ad-blockers have evolved into anti-mining blockers. Execution on the client-side code indeed costs computing power. Numerous variants of this type of economy can be envisioned, replacing advertising by computing contributions, and enabling new redistribution schemes. For now, the economic profitability and the social acceptance of this kind of system seem untested.

Second example: the founder of *Ethereum* himself gives an example of a system "Uberizing Uber": using blockchains and smart contracts, Uber would be decentralized into a collection of unit services, seeking to maximize their individual or collective

effectiveness, or competing with each other. The linking of offers and carpooling requests could be organized in a completely algorithmic way (the latter can also be multi-criteria, e.g. taking into account factors such as proximity, fare, insurance conditions, reputation of the driver and/or the passenger, etc.). Similarly, and more generally, the orchestrating of separate services (e.g. user interface system, research system, road optimization system, payment system, GPS systems, and insurance system) could be implemented via smart contracts (which are temporary objects but objective or automated systems). Smart contracts therefore promise *ad hoc*, opportunistic, flexible and ephemeral "mashups" of highly specialized systems or services. The question of the regulation, existence and management of systemic risks, typical in this type of complex systems, remains an open question.

Blockchains and smart contracts also may play a role in the Internet of Things (IoT) by providing an infrastructure that is programmable - and programmed - for a large number of interacting devices. The Internet of Things holds many industrial promises (for example in logistics and production, but also in the field of aeronautical maintenance). As levers of the IoT, blockchains and smart contracts promise to program and reprogram value chains. Yet, the final mechanisms to be implemented are not known yet (computer security, use of a plurality of blockchains, appropriate proof-of-work if any, etc).

3. Why patenting? The diverse uses of patents

3.1. General reminders

Patents can be offensive or defensive (or both). Granted patents give exclusive rights, i.e. the right to exclude others. A patent is a form of control, i.e. of a decision power, of discretionary options. An effective control often requires multiplying the number of titles. The force of a patent portfolio is generally greater than the sum of the force of its individual members. Patent applications also have advantages, in that they are valuable pending threats on adverse parties (conducting freedom-to-operate analysis, i.e. patent clearances). Applications comprising much - or well hidden - unclaimed matter can be great "weapons". Good knowledge of procedures in the different jurisdictions can optimize the routes to be used (e.g. PCT, national filings, etc). Some tricks exist, like using secondary routes that can stay under the radar of adverse patent attorneys.

When a generic invention is published, specific inventions remain possible. This in particular can imply that improvement patents remain possible, pioneer and improvements possibly neutralizing each other and leading to (undesired) mutual dependencies.

In complement or in substitution to patent rights, defensive publishing can be used. Publication impedes patenting. It can be a poor-man solution but sophisticated defensive publishing can involve a patent attorney, who will for example pay attention to possible adjacent improvements. Internet publications can be used, but preferably,

official "channels" can be used (e.g. early publication of applications before patent offices, natively indexed)

A myriad of other parameters can change the global situation. Patents can change hands. A defensive patent can end up being bought by an aggressive entity, e.g. a patent troll. The technological landscape can change quickly. Patent drafting quality can matter much. Case Law can change, even radically. The amount of text in a patent application can be mobilized more or less appropriately to compete with colliding documents. The period of Examination (e.g. end of the year) can play a role in some jurisdictions. The list goes on.

3.2. Applications to blockchain-related inventions

Bitcoin is (also) a political affair.

In this perspective, it can be valuable to tentatively patent sweet spots, i.e. technological developments that are promising and desirable. But it also can be tactical to patent technological directions that are *not* wanted, at first. You can patent the evil to prevent it and do good. You can patent the good to prevent it and be evil. For example, patents directed towards way to secure the display of advertisements on electronic devices can be filed by opponents to advertisements (to impede ad blockers), or to the contrary, by advertisers to reserve exclusive rights.

Any given filed patent can anti- or pro- Bitcoin. Patenting fundamental aspects are important but secondary features may be as operative (e.g. sidechains, wallets front-end). Patenting sidechains or off-chain scaling, even if undesired technologies for some, can lead to better control and can enable to (re)orient the market (see for example US2016330034).

4. The Particular Case of nChain Holdings (nCrypt, previously EITC Holdings)

Noticeably, a company named nChain Holdings (formerly known as EITC Holdings) is filing numerous patents in the Bitcoin field, for a couple of years. Company nChain is based in London, was incorporated as nCrypt (Private Limited Company) and is supposedly funded at $300 million level. Dr. Craig Wright is Chief Scientist of this R&D entity. Company nChain has published 156 published applications (as of July 2018). Filed after 2014, at least 35 applications have Dr. Wright listed as an inventor. In the corpus of the published *claim trees* filed so far, by excluding common words (e.g. computer, system, message, etc), one can note the use of the following significant words (number of occurrences):

node (528 times), transaction (525), public (396), private (304), script (237), hash (227), value (149), blockchain (147), master (146), secret (130), party (126), metadata (114), token (114), deterministic (102), smart contract (101), crypto-currency (95), cryptographic (84), invitation (81), ledger (81), redeem (81), episode (75), address (66), generator (65), payment (65), content (58), control (41), conditions (34), joining (34), P2P (32), bootstrap (30), elliptic (27), code (25), broadcasting (22), loop (20),

bitcoin (18), traffic (15), handshake (14), attacker (13), gate (13), license (13), profile (12), routing (12), stream (11), mint (10), trusted (10), wallet (10), authentication (9), payroll (8), Boolean (7), rate (7), automaton (6), chain (6), escrow (6), honeynet (6), honeypot (6), fiat (5), random (5), ring (5), risk (5), tree (5), influence (4), tampered (4), interface (3), scanning (3), topology (3), controller (2), irreversible (2), mortgage (2), Turing (2), Merkle (2), Shamir (1).

Titles comprise words or expressions such as:

counting system, secure voting, agent-based Turing complete transactions, feedback, common secret, reactive security, pre-emptive security, choice theory, wallet, P2P, tokenization, scaling of payment, real time, redemption of contracts, web of trust, payroll, consolidated block, secure multiparty, blockchain-enforced smart contracts, peer-to-peer lending, symmetric fair-exchange transactions, logic gate functionality, performance control of a contract, distribution of digital content, ownership verification of software, distributed hash table, peer-to-peer distributed ledger.

Further publications are expected in the near future, but the existing publications provide some preliminary insights.

While it seems that the core protocol is tentatively patented, some words are noticeably absent from claims e.g. "sidechains". Future publications may comprise such words.

Although it is mentioned in the "Satoshi Affair" by A. O'Hagan that nCrypt envisioned to "… *rework financial, social, legal or medical services*", few verticals seem to emerge in the published corpus, to the exception of Digital Rights Management. Likewise, many top words that are strategic in IT are missing, for example: "advertisement" (Google), "cloud" (Amazon) - which is surprisingly mentioned in only seven applications-, or "social" (Facebook, now known to elaborate its future GlobalCoin).

The next section provides ideas of patenting sweet spots.

IV. Perspectives for blockchain related inventions (4/4)

After the provision of definitions, some reminders about patent laws and Case Law, and a rapid analysis of the emerging patent applications, a few temporary conclusions can be proposed with respect to perspectives of blockchain-implemented inventions (i.e. patenting opportunities and open questions).

1. Manifest patenting opportunities

The following remarks shall be considered with extreme caution. No one, except those very intimate with the technology, can know (slightly better) the future sweet spots of the technology.

From our investigations, it seems that patenting opportunities may remain regarding the core technology (e.g. sidechains). Adjacent domains leveraging improvements of enabling technologies (e.g. encryption schemes) may be patentable, by cross-fertilization of technical domains. Specific inventions relating to vertical applications also may be investigated from now on.

1.1. Gaps in core technology (e.g. inventions for scalability)

As the patenting activity on Bitcoin is early, modulo the last 18 months secret period, it appears that important keywords are lacking in the published claims (which define the boundaries of protection).

The case of the word "sidechains" is interesting. In order to scale Bitcoin, and increase its velocity, secondary chains called "sidechains" are sometimes implemented along (main) chains. Some argue that these sidechains degrade security and increase transaction costs. Some others explain that these types of chains introduce deflation (increasing the supply of "money", fractional reserve banking, destruction of the scarcity factor, etc). Sidechains or "off-block scaling" are thus rejected by some in the Bitcoin community. The chief scientist of nChain advocated against them and declared that sidechains were patented. Yet a query with "sidechain" (in the claims), or variants thereof, returns very few hits (e.g. US20160330034, by Blockstream, inventors Gregory Maxwell, Bitcoin Core developer, and Adam Back allegedly inventor of *Hashcash*, see also US20160358165).

This example may indicate that it might then be well possible that pioneer patents still can be taken on generic or broad principles (blockchain e.g. pruning, decentralized consensus mechanisms, advanced smart contracting, etc). As discussed, variants, improvements, alternatives or substitutes to Proof-of-Work systems may also be developed.

1.2. Importation and adaptation of known cryptographic schemes

Cryptography is a major building block of Bitcoin and of blockchains. Improvements in cryptography probably can be "imported" into Bitcoin (i.e. modified and combined, to fit specific technical problems), leading to new patents. In other words, it can be wise to carefully explore portfolios in cryptography (and for example, to study what

inventions are applicable as is to crypto-currency systems, what can be adapted to the underlying economics of crypto-currencies).

As a science, cryptography comprises numerous sub-categories such as Code-based cryptography, Hash-based cryptography, Lattice-based cryptography or Multivariate cryptography. Cryptography is mostly classified in US class 380 or CPC H04L 9/00. The latter class comprises 2242 patent documents. A fraction of the mechanisms described in these patents may be reused and combined in crypto-currency systems.

From a patenting perspective, the list of topics to be investigated is long. A selected list comprises (in no order): *multi-signatures, Shamir's Secret Sharing, secure multi-party computation, information-theoretic security, semantic security, homomorphic encryption, zero-knowledge systems, voting protocols, Merkle signature schemes, ephemeral encryption, Format Preserving Encryption*, etc.

A particular attention may be allocated to quantum computing. To date, the advent of quantum computers is not yet certain, but shall not be discarded. While nChain papers indicate that even with such an advent (e.g. *Shor's algorithm)*, the Bitcoin system wouldn't be threatened, it probably remains worth studying how emerging post-quantum techniques can be used, for example *Quantum Key Distribution* (in the perspective of implementation flaws, which are the sad reality).

1.3. Other adjacent technologies (IP scouting)

The portfolios of *information technology* providers can be explored in depth and, if applicable, be further adapted to the new paradigms. Various adjacent technologies may be mixed-up with Bitcoin fundamentals to improve existing systems (e.g. to improve the *velocity* and the *security* of Bitcoin).

Some key areas comprise security of code implementation, network management, power management, user interfaces, and enabling technologies for derivatives markets.

As *software code implementation* of Bitcoin can be key to security, one may expect patents to address how Denial of Service are addressed, as well as transactions bursts, fault injection, false or malformed or malicious transactions, etc. Generic or specific principles in the field of *computer security* may be combined with existing Bitcoin subsystems to generate new intellectual property. Bitcoin shall be resistant to protocol level attacks (e.g. state-level man-in-the-middle attacks).

Scalability of the Bitcoin network may involve or imply specific network management. Patentable features may be directed towards hardware related inventions, e.g. Power management, GPU computing, FPGA technologies, etc. Originally Bitcoin had no limits for block sizes. To prevent DDoS attacks, a limit has been introduced, later increase and now remains a limiting factor. It is likely that patentable subject matter can be found with respect to scalability.

U*ser interfaces* are keys for the usability of Bitcoin (i.e. velocity of the currency). In addition, patents on user interfaces are detectable from the patent standpoint.

Frontends (i.e. wallets user interfaces) today are recognized as flawed, or not fully satisfactory. The rich portfolios and experience gained in patenting activities of information technology providers is likely to be leveraged for Bitcoin and blockchain related applications. Given the irreversibility of transactions, methods could be developed to reverse, pause, resume, roll back or secure a transaction (against mistakes, misuses, ID theft, etc).

Derivatives markets may well be created on top of Bitcoin. They will, they have to. Such markets can correspond to specific mechanisms. Techniques used in finance for decades can be reproduced "as is", or be specifically adapted. By analogy, the techniques and experience gained in algorithmic finance or High Frequency Trading also probably can be advantageously reused and/or adapted. Patents in finance may be revisited in light of Bitcoin (see for example US9704143).

Patented *computer science* can be scouted, as a general principle, in a high number of directions. For example, with IBM as an assignee, there are 62 patent documents comprising the word "*consensus*" in claims and 481 with the word in specification. Distributed consensus probably can be sophisticated (way more than did Satoshi Nakamoto alone). Virtualization or containerization mechanisms may be investigated to abstract Bitcoin into the meta-management of crypto-currencies competing with each other (Darwinian economics).

Further directions cannot be discussed here.

1.4. Blockchains and inventions specific to verticals

Patenting specific blockchains, and/or applications thereof, may enable the "Internet of Value" (Internet for communication, Blockchain for value. It can be one component of information technology, as many others. Opportunities for patents about the applications of the enabling technologies seem to remain wide open.

Blockchains and other enabling technologies can be used in various industries and for various uses. The ever-growing list of applications of blockchains to various industries comprises to date potential applications in social networking, in manufacturing (e.g. avionics, logbooks), in robotics, in utilities e.g. management of smart grids, in media (e.g. Digital Rights Management, distribution of contents), in services (e.g. insurances), in travel industries (e.g. ticketing), in legal services (e.g. electronic negotiation), in education, in healthcare (e.g. patient record management), by governments or public services, for personal security, identity or safety, in logistics (e.g. transportation), in telecommunications, and even in gaming (Internet betting, Bitcoin has roots in casinos).

Each of these verticals may require specific combinations of Bitcoin-related technologies, some of them being possibly patentable. In some cases, some of these specific developments may enrich general principles in return.

For example, an Internet of Things relying on blockchains may present very specific technical problems and thus solutions. Such solutions may involve nano-transactions, use *Physically Unclonable Functions* (hardware functions for example to perform challenge-response tests), etc.

Privacy management techniques relying on blockchains may implement one or more mechanisms such as *k-Anonymity, l-diversity, Virtual Party Protocols, Secure Sum Protocols, differential privacy, exponential mechanism, quasi-identifiers, or Statistical Disclosure Control.* Many other applications may be cited, e.g. in data analytics, machine learning (e.g. deep, federated, etc).

Another area of interest is the intellectual property of "merchants", for example of Amazon (see US8719131), or Wal-Mart. Merchants have an incentive to provide the hash power to run blockchains properly (they want to get paid). It seems that patent filings are rapidly increasing on their end.

2. Open questions and horizons

Bitcoin and associated emerging technologies raise numerous fascinating questions. Most of these questions may raise interests to take control i.e. can be addressed in patent applications. In no order:

Going large. If and when scaling according to Moore's Law, could millions of blockchains compete or otherwise cooperate (similarity metrics, etc)? Hybrid systems of decentralized and "centralized" (i.e. databases) blockchains may emerge, and be patented. Artificial Intelligence (A.I.), in practice Machine Learning, often leverages on "Big data". How do blockchains relate to "A.I" and/or "Big data"? Does A.I. need blockchain-secured data?

Going small. Can blockchain methods and systems be applied to the lowest computing scales in space and/or time (e.g. at instruction level in a CPU)? The Internet of Things also may use specific type of blockchains or Proof-of-Work schemes.

Going meta. Coins are inextricably bound to their protocols (OSS). Would it be possible to orchestrate coins (master-coin, etc)?

Going upstream. May some existing cryptographic techniques be revisited according to present new perspectives, to better adjust current needs?

Going downstream. What opportunities for blockchain analytics i.e. observing blockchains?

Going business. New business models, now with a cryptographic flavor, may become possible and patentable (micro-transactions, new types of intermediaries or data brokers, etc).

Going political. Nations and government do enact laws. While some countries are favorable to digital currencies (Bitcoin has got official blessing in Japan in April 2017), many other turn their back to them (e.g. China). The diversity of attacks is increasing

(lastly, the Bitcoin blockchain has being alleged to comprise hyperlinks to videos of child abuse). Bitcoin has to make its way through many regulations, e.g. banking regulation, social acceptance, economical and ecological relevance. Patent laws may be changed, so as Case Law, in favor (e.g. tangible i.e. cryptographic "flavor") but also in disfavor of crypto-currencies (e.g. reduction to practice).

To protect your intellectual property, contact algopatent.com