# Cryptocurrencies, Blockchain and Risk Management:

## Legal, Operational and Systemic Risks

Ann Sofie Cloots

*PhD Candidate, Faculty of Law*

Centre for
**Risk Studies**

UNIVERSITY OF CAMBRIDGE
Judge Business School

McKinsey&Company

# 2018 Cambridge - McKinsey Risk Prize

# Bio-sketch and Photo Page

**Student Name:** Ann Sofie Cloots

**Email contact:** ascc2@cam.ac.uk

**Title of Submission:** Cryptocurrencies, Blockchain and Risk Management: Legal, Operational and Systemic Risks

**I am a candidate for the degree:**

PhD, Faculty of Law

Bio-sketch (Approximately 150 words)

I am a PhD candidate at the Faculty of Law, researching how the legal model of the company, the economic model on which it is based, and management theory can be reconciled. Company law is based on certain economic assumptions about human behaviour and motivation, which may differ from assumptions reflected in management scholarship.

My research interests broadly cover corporate governance, law & economics, behavioural studies, quantitative legal methods, legal theory and philosophy as well as the legal implications of fintech.

After finishing my Masters, I pursued an LLM in the US, focusing on public international law and political philosophy. I gained corporate and competition law experience as an associate in two US-based law firms.

Centre for
**Risk Studies**

UNIVERSITY OF CAMBRIDGE
Judge Business School

McKinsey&Company

# 2018 Cambridge - McKinsey Risk Prize

# Declaration Form

**Student Name:** Ann Sofie Cloots

**Email contact:** ascc2@cam.ac.uk

**Title of Submission:** Cryptocurrencies, Blockchain and Risk Management:

Legal, Operational and Systemic Risks

**Number of words of submission:** 5353

**I am a candidate for the degree:** PhD

**Academic Institution/Department:** Faculty of Law

**Declaration**

I confirm that this piece of work is my own and does not violate the University of Cambridge Judge Business School's guidelines on Plagiarism.

I agree that my submission will be available as an internal document for members of both Cambridge Judge Business School and McKinsey & Co's Global Risk Practice.

If my submission either wins or receives an honourable mention for the Risk Prize, then I agree that (a) I will be present at the award presentation ceremony 20 June 2018, (b) my submission can be made public on a Cambridge Judge Business School and/or McKinsey & Co websites.

This submission on risk management does not exceed 10 pages.

Signed (Electronic Signature)

*Ann Sofie Cloots*

Please include this declaration form after the cover page of your paper submission.

**Abstract**

This paper is about legal risks, as well as a number of operational and systemic risks, associated with the acceptance and use of cryptocurrencies and the blockchain technology. The paper consists of five parts. After an introductory section 1, section 2 analyses the main legal risks of cryptocurrencies, in particular the risk that tokens may be re-qualified retroactively as securities by regulatory agencies. Section 3 assesses the legal risks of blockchain, the technology underlying cryptocurrencies, in particular the compliance risks flowing from the much-discussed EU GDPR. Section 4 discusses a number of operational and potential systemic risks of cryptocurrencies and blockchain technology. Section 5 concludes with a number of practical takeaways for risk managers.

## 1. Introduction

Cryptocurrencies, and the blockchain-technology underlying them, need no introduction here.[1] Cryptocurrencies ('coins' or 'tokens'), were defined in Satoshi Nakamoto's famous 2008 paper as "a purely peer-to-peer version of electronic cash" that allows "online payments to be sent directly from one party to another without going through a financial institution".[2] Rather than relying on a financial intermediary, such payments rely on trust: trust in an algorithm, not any particular individual or institution. The most well-known cryptocurrency is Bitcoin,[3] although in the meantime hundreds of cryptocurrencies exist.[4] Blockchain is the distributed ledger technology underlying cryptocurrencies. The bitcoin distributed ledger is the earliest and most well-known one, although the ethereum ledger has surpassed it as the most used distributed ledger.[5]

The discussion continues on whether either cryptocurrencies or blockchain technologies are more likely to revolutionize our societies. Those who sympathize with the Cyberphunk movement, as well as those from countries with volatile fiat currencies and high inflation, may think cryptocurrencies are the true innovation, with its potential to replace or at least challenge the centuries-long dominance of governments over minting. Others take the view that cryptocurrencies will never be more than a fringe phenomenon and that the real innovation and efficiency increase lies in blockchain technology.

The working assumption for this paper is that the disruptive potential of both cryptocurrencies and blockchain is significant, although the risks and weaknesses of both are easily lost in the hype surrounding them. The next sections aim to identify the main such risks and weaknesses to help see the forest for the trees.

---

[1] For a general introduction to the technology, see the free online Coursera course "Bitcoin and Cryptocurreny Technologies" offered by Princeton University. NYT-journalist Nathaniel Popper wrote an excellent book about the genesis and early days of Bitcoin and the Cyberphunk movement, *Digital Gold*.

[2] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", Nov. 2008, https://bitcoin.org/bitcoin.pdf.

[3] Some of the precursors to Bitcoin are described in in Popper's *Digital Gold*, see note 1.

[4] The Coin Market Cap website lists over 1500 cryptocurrencies and websites such as ICOSource list ongoing and upcoming ICOs. The main exchanges limit the number of tokens that can be traded, with Coinbase trading only 3 cryptocurrencies and Bittrex 190+ tokens.

[5] The ethereum *ledger* has the greatest number of applications built upon it. When it comes to the *cryptocurrency*, however, the Bitcoin token still has a larger market capitalization than Ether, although Ether temporarily surpassed Bitcoin in trading volume in March 2017 (it has meanwhile been surpassed again by Bitcoin).

## 2. Legal and compliance risks of cryptocurrencies

The literature on the legal risks of cryptocurrencies and the underlying blockchain technology is still in its infancy, though growing at rapid pace. The first relatively comprehensive legal handbook in this field is yet to be published[6] and is likely to be outdated as soon as it rolls of the printers. The main legal risk identified and discussed by practitioners and academics so far is the **risk that tokens will be reclassified as securities** by security regulators and enforcement agencies worldwide.

Cryptocurrencies have proliferated over the past year through token sales or so-called ICOs, even surpassing VC funding in the blockchain space (*Figure 1*).[7]

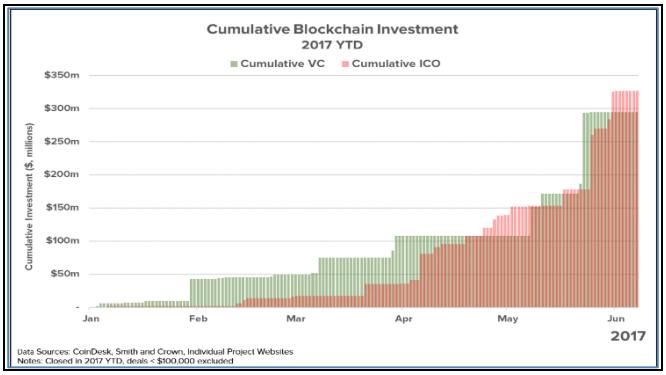


**Figure 1: VC and ICO funding in blockchain. Source: Coindesk.**

Originating as a fringe phenomenon, ICOs have caught the attention of regulators worldwide in the course of its stellar expansion in 2017 (*Figure 2*). ICOs raised around US$3 billion in 2017 and the average ROI of ICOs launched in 2017 was over 1,200%.[8]

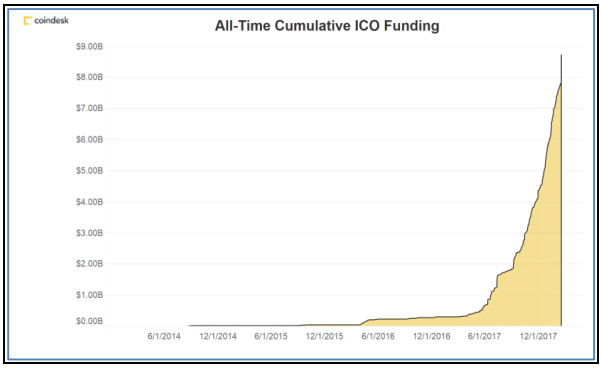


**Figure 2: ICO Funding 2014-2017. Source: Coindesk.**

Regulators' reactions have been mixed.[9] In some countries, such as China and South Korea, ICOs have been banned outright. Most other countries have threaded more cautiously in an attempt to balance the two-fold aim of allowing this nascent technology to develop and companies to experiment, while

[6] P. de Filippi and A. Wright, *Blockchain and the Law: The Rule of Code*, Harvard University Press, forthcoming.
[7] ICO stands for Initial Coin Offering. The term was coined in reference to the traditional securities sale known as IPO or Initial Public Offering.
[8] https://www.coinist.io/ico-roi-2017.
[9] For a large-scale overview of government policies towards cryptocurrencies, see http://bitlegal.io.

protecting the investing public from outright fraud and scams. Most jurisdictions have warned both the public and cryptocurrency companies that token sales through ICOs can fall under traditional securities regulation, although enforcement of securities regulation has been highly limited so far and focused mostly on outright scams or blatant violations of securities laws.[10]

Indeed, anyone vaguely familiar with securities regulation and regulators' willingness to apply existing laws to new technologies would have deemed it naive to think that merely replacing a traditional security for a token, or using the term ICO instead of the familiar IPO or 'SAFT'[11] rather than 'SAFE' would suffice to escape regulatory scrutiny. Even though enforcement so far has been limited, there are sufficient warning signs that regulatory agencies are keeping a close eye on the sector and stand by to step up enforcement whenever it is deemed desirable.[12] Even though enforcement may be limited as of yet, this does not prevent regulators to enforce securities regulation retroactively. This means that no ICO is completely safe from retroactive criminal sanctions and civil damages. So far, with one exception, no ICO has made an attempt to comply with securities regulation. Hacker and Thomale found no trace of an ICO offered in the EU that complied with EU securities regulation.[13] Moreover, even if regulatory enforcement is limited, the risk of civil litigation is tangible: nothing prevents an investor in an ICO to claim civil damages in court for any breach of securities regulation.[14] It will be up to courts to make a case-by-case assessment of whether a token sale was, in fact, a security issuance in disguise. It is likely that most judges will be relatively unfamiliar with the fast-changing token environment and will find little guidance in either regulatory briefs or academic literature, both of which are still quite limited (the former more than the latter). The so-called White Paper that is typically published in anticipation of an ICO, any promotional materials for the token sale as well as the actual investment contract (whether a 'SAFT' or other), will form the basis for the factual assessment of whether a token was in actuality a security.

Regulatory guidance so far has been rather generic, especially in the EU. Practitioners and academics have nevertheless much refined the binary question of whether tokens are currencies or securities, to a much more nuanced discussion on which types of tokens are likely to constitute securities and which ones are not.

The consensus has emerged that tokens may well be covered by traditional securities regulation, though a case-by-case analysis is required to verify whether any particular token is. Different broad categories of tokens have been identified in the legal literature (utility (or app) tokens, protocol tokens, currency tokens, investment tokens), with the legal re-classification as a security higher depending on the type. Is the token required to gain access to a particular application (e.g., Filecoin)? Can tokens be sold immediately after the ICO? Will the token sale be used to finance the development of a particular decentralized app (dApp) or is the dApp already fully operational? Is the token sale advertised through a

[10] In the EU, see ESMA's warnings for ICO investors and firms (13 November 2017). No enforcement action has been taken so far (see Hacker and Thomale, note 12 and 22). In the US, the SEC has put ICO issuers on warning and took a limited number of enforcement actions. See "Statement on Cryptocurrencies and Initial Coin Offerings" by SEC Chairman Jay Clayton, 11 Dec. 2017; see also the investigative report on the DAO (25 July 2017) and enforcement actions against cryptocurrency firms AriseBank (16 Feb. 2018) and Bitfunder (21 Feb. 2018).

[11] See note 15 below.

[12] See ESMA's 2018 Risk Management Working Programme.

[13] Hacker and Thomale (below, note 22) found no trace of an ICO offered in the EU that complied with EU securities regulation ADD Hacker article. An exception is Filecoin, which structured its ICO as a private placement under US law (*id.*)

[14] *Id.*

so-called SAFT[15]? A token issued prior to the dApp development, based on a SAFT and promoted as capable of generating high returns on investment is more likely to be reclassified as a security in the US.[16]

The difficulty arises with tokens that serve a dual function, for example tokens that can serve both as a way of accessing a service offered by a particular dApp, but that can also be freely traded on a coin exchange and can form the object of speculation (e.g., Filecoin as a service and the Filecoin token). If the current regulatory response towards ICOs continues, such dual-use tokens are likely to have less enforcement priority than outright speculation or investment tokens. Regulators or courts may carve out safe havens for dual-use tokens that can demonstrate that the token also materially serves as a building block for a particular protocol (distributed ledger) or access tool for a particular dApp (utility token), in addition to being actively traded.

In the US, the Supreme Court defined a security in the 1946 *Howey* case. Most legal commentators agree that *Howey* will allow to reclassify at least certain tokens as securities.[17] The Supreme Court of Canada uses a definition of security that very closely resembles the *Howey* test. In the EU, the definition of a security is contained in the Prospectus Directive. ESMA guidance is generic and legal commentators anticipate that at least investment tokens are very likely to be covered by the Prospectus Directive and its disclosure requirements.

Is there any **risk for companies or individuals accepting crypto-payments** for goods and services, such as Expedia or Microsoft? The risk of legal ripple effects of a token reclassification on companies accepting that token as a payment tool at present seems rather distant (though this of course depends on the jurisdiction). Legal risks from accepting cryptocurrency payments are more likely to flow from the anti-money laundering (**AML**) and know-your-customer (KYC) laws applicable to financial institutions and professional service firms assisting them (such as auditors or lawyers). Tokens are held in virtual wallets and transactions can take place either between wallets directly or can be mediated by an exchange. Wallets can be anonymous (most wallets are), making cryptocurrency trading a convenient tool for fraud, tax evasion, evasion of international sanctions, the sale of illicit goods and services and money laundering.

Exchanges such as Coinbase or Bittrex[18] have anticipated such compliance risks and impose customer identification requirements as a precondition for trading cryptocurrencies (or converting them into fiat money). These are only partial solutions, not only because both exchanges have encountered their own teething problems (leaving Bittrex unable to register new customers due to scaling problems, while Coinbase customers recently saw their trading capacity severely limited due to problems with the platform's infrastructure, which, due to the high volatility of cryptocurrencies, can lead to substantial losses). Moreover, many other exchanges impose no or highly limited identification requirements, facilitating anonymous trading. In addition, even where trading would be de-anonymized or pseudonymized, wallet-to-wallet exchanges largely escape any form of formal identification. This makes it difficult for banks and companies accepting cryptocurrency payments (especially where tokens can be exchanged for fiat money) to genuinely know the origin of the funds accepted. Accepting what may be the proceeds of fraud, corruption, money laundering, terrorist funds or tax evasion without sufficient due diligence comes with its

[15] "Not so fast – Risks related to the use of a "SAFT" for token sales", Cardozo Blockchain Project, 21 Nov. 2017, in reaction to Batiz-Benet, Clayburgh and Santori, "The SAFT Project: Toward a compliant token sale framework".
[16] See, e.g., Rohr and Wright, Draft Research Paper, Dec. 2017, SSRN ID3048104 (work in progress).
[17] Not everyone agrees that the *Howey* test will be successful in token reclassification, see e.g., Robinson, "The New Digital Wild West: Regulating the Explosion of Initial Coin Offerings", Jan. 2018. SSRN ID 3087541.
[18] See https://www.coinbase.com and https://bittrex.com.

own legal risks, if not criminal (aiding and abetting a criminal enterprise, complicity in corruption) then civil liability risks (seizure of the proceeds of money laundering, terrorist funding or schemes to circumvent international sanctions). Even though there may be no examples yet, a lack of due diligence as to the origin of cryptopayments accepted by a potential takeover or merger target should feature on the **list of representations & warranties of M&A dealmaking**.

### 3. Legal and compliance risks of blockchain technology: the EU GDPR

This section looks at the legal risks associated with the use of blockchain technology by a company or a consortium of companies. There are a number of such risks that have yet to be fleshed out in practitioners' or scholarly analysis. Due to space constraints this section will focus on one main risk, namely the risk of a violation of the much-discussed General Data Protection Regulation ("**GDPR**") in the EU. Violation of the GDPR is of potential concern not only for EU-based companies: any natural or legal person processing personal data of individuals in the EU for professional or commercial reasons falls within its scope. The GDPR explicitly states that its scope is independent of the technology used for the data processing. GDPR concerns are relevant both for token sales (discussed above) as well as for the commercial usage of blockchain technology. Whereas ICOs have often avoided US investors due to legal uncertainty about the applicability of US securities law to token sales, ICOs have typically led to sales of tokens to EU investors, making GDPR concerns highly relevant.

Beyond token sales, a sizeable number of companies are experimenting with, developing or already using blockchain technology (such as Walmart or Maersk). This can be in the form of an open (or permissionless) blockchain or a private (or permissioned) ledger. The most well-known ledger, the bitcoin blockchain, is permissionless: any user of an electronic device capable of running the ledger can join the network (becoming a 'node' of the distributed network). Nodes can become 'miners': they can contribute hashing power to solve equations required to 'mine' the next block on the blockchain. Mining a block leads to a reward for the miner who won the race to solve the equation puzzle to form the next block, at least if the blockchain is set up to reward so-called 'proof of work' (almost all blockchains are set up this way). Proof-of-work blockchains (such as the bitcoin blockchain or the ethereum ledger) are highly energy-intensive, which has caused public outcry over their environmental footprint. For companies, such high energy usage risks leading to a negative analysis from ESG-investors. As an alternative to the energy-intensive proof-of-work reward system, there have been increased efforts to shift to a 'proof-of-stake' system, which lowers energy use substantially. Ethereum's attempts to develop a proof-of-stake alternative with its Casper project has run into substantial development obstacles. The Cardano Foundation is working on a competing version of a proof-of-stake blockchain, which is a more viable alternative for companies conscious of the **environmental and reputational risks** associated with the energy-intensive proof-of-work blockchains currently dominating the field.

The difference between a permissioned and permissionless blockchain matters for the compliance risks with the EU's GDPR. How does the GDPR apply to blockchain users?[19] Under the GDPR, a controller or processor of private data has to comply with its stringent data-protection requirements, such as ensuring a right to data access, data correction, data transferability and the right to be forgotten. For a permissionless distributed ledger, compliance risks are higher than for a permissioned ledger.

[19] For an excellent analysis of the potential implications of the GDPR for blockchains, see M. Finck, *Blockchains and Data Protection in the European Union*, Max Planck Institute for Innovation and Competition Research Paper No. 18-01, on which the legal analysis in this section is based.

**Pseudonymization of data is insufficient to protect data privacy**, as confirmed by EU courts for pseudonymous IP addresses**. Most blockchains, however, use a form of pseudonymous cryptography.** While proponents of bitcoin and other blockchains often hail the ledger's claimed anonymity, most blockchains leave traces of a user's identity that are visible to other users. To understand how this is possible, it is necessary to understand the basics of public-private key encryption used for blockchain cryptography. Each user receives a public and a private key associated with the user's unique wallet. These keys are randomly generated through an algorithm. However, the public and private key are mathematically linked: a specific public key will generate a particular private key. A user shares his public key for transactions, but should never share the private key. Most blockchains include public key information in the chain for verification purposes, which is visible to all users. Since the private and public key are algorithmically linked, sharing your public key gives a minuscule hint of your private key (by itself almost computationally intractable). If combined with additional identifying information, the public key may give away a user's identity. For example, a third party can look at the blockchain to identify all transactions made from a particular virtual wallet. If usage of a wallet reveals the IP address from which the transactions have been made, a user's identity may be revealed indirectly. Even bitcoin users have been traced combining the public key of their wallet with other identifying traces left on the blockchain.

A pseudonymous blockchain that allows a third party to trace the identity of a user violates the GDPR.[20] A company like Zcash allows blockchain transactions that are fully anonymous. If used on a permissionless blockchain without further identity checks, Zcash's technology may be compliant with GDPR requirements, but is likely to run afoul of the AML and KYC requirements imposed by other laws. Combining Zcash's anonymous technology with a permissioned (closed) blockchain mitigates the legal risks of both GDPR and AML violations. Moreover, for blockchain applications in a consortium, this limits the risk that commercially sensitive information is shared with competitors (which in turn limits risks of cartel allegations). This is presumably the reason why JPMorgan entered into a partnership with Zcash.

In the context of a blockchain, it is unclear who is the processor and controller of private data. Is it any node that runs the software? If so, the EU's enforcement agencies could in theory fine any single owner of a device that runs the ethereum, bitcoin or any other pseudonymous blockchain software. This not only seems politically undesirable, but also practically unfeasible, at least for widely dispersed, permissionless blockchains. Or would EU enforcers target miners, as data processors or controllers? Although more concentrated than nodes (see below), there are still a large number of miners that make such action difficult to implement (especially since the largest mining pools are located in China and other non-EU countries).

Based on an educated guess, it is feasible that the Court of Justice of the EU's (CJEU) proportionality principle may prevent it from imposing a disproportionate burden on any node (potentially even every miner) in a permissionless blockchain like bitcoin or ethereum. The Court may well weigh the repercussions of using a blockchain on a user's right to privacy against the repercussions of imposing the full force of the GDPR on every user-node. For a permissioned blockchain, however (the majority of the commercial blockchains being developed), it is easier to identify data controllers and processors and therefore it is more likely that the GDPR requirements will be more vigorously enforced there. For a consortium-based blockchain such as R3's Corda, the risk of GDPR compliance is lower if only data from the consortium members are stored on the blockchain. As soon as third party data is stored on the ledger as well (such as data of the consortium members' customers or suppliers), GDPR compliance risks increase.

[20] *Id.*

For consortium-based blockchains, there are furthermore the standard **competition law risks**: any cooperation between competitors (including the development of a shared blockchain) needs to stay clear of anti-competitive behaviour. The development of a shared blockchain between competitors needs to ensure that **no commercially sensitive information is shared**. The higher the collective market share of the competitors involved, risks of market abuse may also arise, depending on whether non-members can join the consortium and under what conditions. De facto exclusion of minor players from a consortium led by the industry's market leaders, or inclusion only at unreasonable conditions or unreasonably high entry fees can fuel claims of artificially erecting barriers to entry in contravention of competition laws. This risk is well-known to competition lawyers and is not novel, although a lack of understanding of the blockchain technology and the type of information shared on such distributed ledger (including digital fingerprints that can indirectly help identify transacting parties) between competitors may limit risk managers' potential to genuinely assess compliance risks.

Companies may be tempted to increase the efficiency and timeliness of deal-making or corporate transacting through "**smart contracts**". Although there has been some discussion on whether smart contracts are contracts, the consensus is that they are.[21] This means contract law requirements of the relevant jurisdiction need to be complied with to ensure validity and enforceability of the contract. Some scholars have argued that smart contracts are a *lex cryptographica* that would make default contract law provisions redundant, as the code would be the full law between the parties. This is highly unlikely: international private law treaties or regulations will typically provide sufficient clues for a legal 'hook' to identify jurisdictional competence of a particular legal regime. A more pressing question for legal risk managers is **how code and prose contract terms will be weighed** by courts: in case of an unforeseen difficulty in the implementation of the code or the interpretation of the contract terms, will the code have priority over the written contract terms? Will lawyers involved in the deal-making bear legal responsibility for code errors? Will courts be sufficiently equipped to understand the interplay between the complex code and the written contract? Of course, a contract can anticipate many of these issues, although it ultimately remains up to the courts to decide on the validity and enforceability of any contractual terms as well as interpret existing laws in light of smart contract technology. In view of the lack of reliable legal precedents, and arguably a lack of familiarity of courts with the minutiae of smart contract functioning, risk managers should adopt a precautionary stance.

## 4. Operational and systemic risks of cryptocurrencies and blockchain

The early adoption of cryptocurrencies by the so-called Cyberphunk movement[22] was largely because of its promise of a decentralized money tool: whereas fiat money depends on the state, cryptocurrencies were hailed as a form of value storing tool that does not rely on the government. Beyond the ideological appeal to those early adopters, there was a practical appeal for those living in countries where government policies caused skyrocketing inflation or severely limited capital outflow.

A decentralized ledger is decentralized in the sense that the ledger is shared and run by a potentially very large number of nodes. However, *mining* has become very much concentrated, as shown by *Figure 4*:

[21] See, e.g., Werbach and Cornell, "Contracts Ex Machina" (2017), SSRN ID 2936294.
[22] See Popper's book *Digital Gold*, supra, note 1.

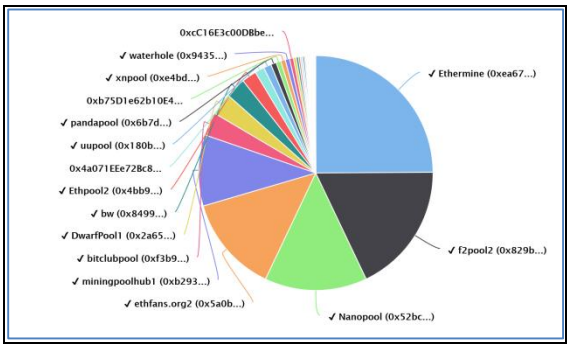


**Figure 3: Concentration of miners. Source: Etherchain, 28 Feb. 2018**

For most blockchains (those operating on a proof-of-work basis), **concentration of mining power** means concentration of voting power. The governance of the blockchain of, for example, bitcoin or ethereum is decided upon by 50%+1 of the mining power. This means a consortium of two or a few of the largest miners can change the algorithm of the blockchain to their advantage. Such concentrated mining power goes against the very idea behind the blockchain, namely as a mathematical solution to the Byzantine Generals problem.[23] For a company building an application on the bitcoin or ethereum blockchain, the concentration of mining power increases the risk that a collective of miners changes the underlying code (which may lead to so-called soft-forks or hard-forks of the ledger and any tokens associated with it) to the detriment of the company.

Investment in ICOs has boomed over the past year, although the market capitalization of all tokens combined is still dwarfed by that of traditional investment instruments (the aggregate worldwide value of stocks alone is already several dozen trillion)[24]. The risk that a breakdown of the cryptocurrency ecosystem would pose a systemic risk to the wider financial and economic environment is, as of yet, limited. Nevertheless, the stellar speed with which this ecosystem expands requires one to be aware of the potential systemic risks that can arise in the relatively near future, in particular now that derivatives such as bitcoin future contracts can be traded on markets like CBOE and CBE.

For now, however, such **systemic risks are low**. A more pressing risk is that of the **increasing use of a limited number of ledgers, in particular the ethereum blockchain, for a large number of tokens and dApps** (including smart contracts[25]), both permissioned and permissionless. It is much harder to find reliable statistics on the use of the ethereum *ledger* as opposed to the transactions of the Ether *coin* (see note 5).

[23] The Byzantine Generals problem is a mathematical fault tolerance concern. Put simply, in this context it means: how many nodes in the blockchain can go rogue before the system collapses? For a more technical description, see http://www-inst.eecs.berkeley.edu/~cs162/fa12/hand-outs/Original_Byzantine.pdf.

[24] https://data.worldbank.org/indicator/CM.MKT.TRAD.CD?end=2016&start=1975&view=chart

[25] Hacker and Thomale, "Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law" (2017) noting AXA's use of the ethereum chain for insurance claims.

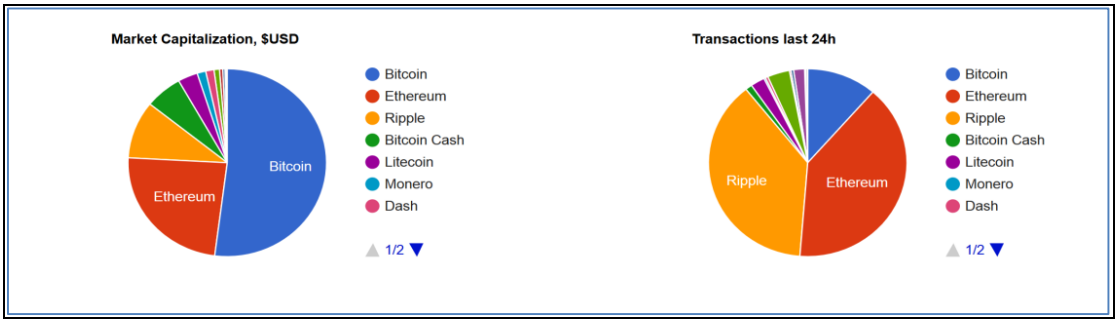


**Figure 4: Tokens by market capitalization and by transaction volume. Source: BitInfoCharts, 2 March 2018**[26]

Any vulnerability of that ledger, in particular any cryptographic security concern, can result in a negative downward spiral in the token and dApp ecosystem. The market-share of ethereum, much like bitcoin, makes it an especially valuable object of attacks for hackers. This is a potential systemic risk for the young but booming ecosystem of tokens and dApps, which is built on trust in the underlying cryptographic algorithms. This risk is tangible for both permissionless and permissioned blockchains, as well as for any company issuing or accepting cryptocurrency payments. News of security concerns with either the bitcoin or ethereum ledger can have spiraling effects on token pricing and on the liquidity of token transactions. While distributed ledger technology is more secure from hacking than concentrated hacking, the typically open-source coding is visible for anyone to see, including for hackers who can take the opportunity to identify and exploit any weaknesses in the code. Since there is no central company behind a distributed ledger, no one is in charge to fix a bug or force a patch onto all nodes (nodes can refuse to implement a code update).[27] Furthermore, the requirement that code updates are accepted by a majority of miners can cause material delay in the implementation of an updated version of the code. Even though blockchains are often claimed to be 'tamper-proof' or 'irrevocable', they are not. At most they are tamper-resilient. Altering previous blocks requires a high degree of computational power, but it is not impossible. Understanding this basic feature of the technology is tantamount to an adequate risk-mitigating strategy.

## 5. Conclusion: Practical takeaways for risk managers

The paper has identified a number of legal risks for both cryptocurrencies and blockchain technology, as well as a brief discussion of some major operational and potential systemic risks. The main takeaways for risk managers are summarized below:

- Regarding cryptocurrencies, the main legal risk is the **reclassification** of a sizeable number of tokens as securities. Any ICO requalified as a security issuance and not compliant with stringent securities regulations can lead to criminal sanctions for the organization and individuals behind the token sale (and potentially anyone else facilitating such sale, depending on the jurisdiction) as well as civil liability. Whereas enforcement so far has been non-existent or limited (targeting blatant violations or fraudulous scams), stricter enforcement is high on the radar for enforcement agencies in many of the key jurisdictions (see, e.g., ESMA's 2018 Risk Assessment Work Programme).
- Further legal risks of cryptocurrency sales and transactions are violations of **anti-money laundering laws** for financial institutions. Not only banks, but also any company accepting cryptopayments (or

[26] Note, however, that volumes recorded by https://coinmarketcap.com/currencies/volume/monthly/ come to a different conclusion (placing BTC and USDT ahead of ETH).
[27] Walch, "The bitcoin blockchain as financial market infrastructure: A consideration of operational risk" (2015).

allowing cryptocurrencies to be exchanged for fiat money, which regulators in countries like China have been especially suspicious of) should engage in proportionate due diligence to mitigate legal risks, such as potential criminal or civil liability for complicity in **tax evasion, circumvention of international economic sanctions, funding of terrorist organizations or corruption** (in particular the wide jurisdictional reach of the US Foreign Corrupt Practices Act).

- Legal risks associated with cryptocurrencies can further expand to derivatives of such tokens, such as the recently approved futures contract market of the CBOE.
- Companies applying blockchain technology to any part of their operations, and who offer goods and services in the EU, need to be aware of the compliance risks regarding the EU's **GDPR**. Political and practical reasons may prevent regulators to vigorously enforce the data protection rules to nodes in widely dispersed, permissionless blockchains. It may nevertheless be enforced against miners. Moreover, permissioned blockchains with a limited number of participants may find themselves more easily targeted by the GDPR (fortunately, it is also more feasible for such ledgers to comply with the Regulation). Blockchains that make public keys of users visible (the majority of ledgers at present) cannot guarantee the anonymity required under the GDPR. A sector-wide code of conduct or certification mechanism can be considered as a mitigating circumstance in case a violation of the GDPR is deemed to exist.
- Consortium-based permissioned ledgers between competitors need to be aware of potential **cartel** and **market abuse** legal risks. These risks are not new, but insufficient knowledge of the technology may lead risk managers to underestimate the extent to which **commercially sensitive information is shared** or barriers to entry are erected for non-members of the consortium.
- For those overseeing M&A deal-making, awareness of the legal and operational risks of cryptocurrencies and blockchain technology is required in order to include adequate protection in the **representation & warranties** documents of the deal. This calls for a basic understanding of the technology by risk managers, including blockchain-based smart contracting used for deal-making.
- Operational concerns include the **concentration of mining power** and potential change of the underlying code to the detriment of companies using a particular blockchain technology for their operations. The open-source code gives hackers an advantage to identify weaknesses in the code and the lack of centralized party in charge may delay an adequate response to security concerns. The **concentration** of token sales and dApps **on the ethereum blockchain** means an increased vulnerability of the ecosystem to any operational (e.g., transaction speed or scaling issues) or security problems with this ledger technology.
- The best risk strategy towards cryptocurrency and blockchain related risks starts from an understanding of the basic technology. Fortunately, an increasing number of tools are available to help risk managers face this challenge.[28]

[28] In addition to the Cousera course offered by Princeton mentioned above (see note 1), the Khan Academy offers a number of free online tutorials on the basics of cryptography, https://www.khanacademy.org/computing/computer-science/cryptography.