KING'S College LONDON

Blockchain and Trade Secrets: A Match Made in Heaven?

Sindre Dyrhovden

Abstract:

The urge for digitalisation in the 21st century is creating a fully electronical environment where every aspect of a business is computerized, and a voluminous size of information is stored in high-density electronic media. Together with the high degree of employee mobility in today's globalised economy, this has made the trade secret holders experience the shadow-side of digitalisation as the risk of trade secret theft is more emerging than ever. This pattern has come parallel to the development of new technology for the purpose of securing digital information. Blockchain and related distributed ledger technologies, have taken the digital space by storm, redefining technological efficiency in a number of industries and for a number of purposes. Considering that this technology could create a secure, time-stamped, incorruptible chain of information, this paper will explore the potential of, and alternatives to minimise the downsides of digitalisation for trade secret holders, in a time where the protection of trade secret has become more relevant than ever.

Table of Content

I. Introduction

In a time where 80% of the value from the fortune 500 companies consists of intangible assets, is it safe to say that protection of intellectual property has arisen as the number one priority for private companies and governments.[1] However, in the ever-growing electronical environment for intellectual property it is constantly getting harder for owners to secure their assets.

The major upheaval in digitalisation in the two last decades has especially affected the use of trade secret protection for intangible assets. Traditionally, innovations have mainly been protected with patents as long as the requirements were fulfilled. Nevertheless, in line with the growth in new technology, the use of trade secret protection is seen to mirror the very same exponential curve of growth (*figure 1 below*). This is not a coincidence as protection through secrecy is flexible and fits the full range of innovations in the 21th century. However, the consequence of the 'secrecy' in trade secrets, is ironically that the very same technology makes modern trade secret protection a critical and vulnerable area of intellectual property rights. With the great value of intangible assets and considerable increase in employee mobility and digitalised data storage, the risk of trade secret misappropriation has become bigger than ever. The revolution in information technologies has not only made it easier to access confidential information, but additionally makes it possible to transmit huge amounts of data with the click of a button. These emerging issues in trade secret protection is illustrated through the fact that economical loss from trade secret theft in the US singlehandedly is estimated to constitute as much as 1-3 % of the US GDP.[2]

The traditional means of securing trade secrets by notarizing documents and hiding them away in physical safes for decades at the time, is long gone. There is an essential need for new-thinking and efficiency measures in trade secret protection to make it easier for trade secret holders to establish ownership rights and demonstrate compliance with the legal requirements in a newly found digital environment. Blockchain, or distributed ledge technology (DLT) has, in the last decade, broken free from its shell in the financial sector and is proving to be of major value in several new areas of business every day. The value of blockchain technology for the purpose of trade secret protection, lies in its immutable and transparent character. Blockchain

[1] Vivek Mani and Sachin Sancheti, 'Economic Approaches To Remedies In Trade Secrets Cases' (*Cornerstone.com*, 2016) <http://www.cornerstone.com/Publications/Articles/Economic-Approaches-to-Remedies-in-Trade-Secrets-Cases> accessed 9/05/2019.

[2] *Reasonable Steps" To Protect Trade Secrets: Leading Practices In An Evolving Legal Landscape' (Create.org, 2015)<https://accounsel.com/wpontent/uploads/CREATe_org_Trade_Secrets_Reasonable_Steps_7_15_15_Final.pdf> accessed 04/07/2019. 2.*

technology can create a secured timestamped and immutable chain of information which can prove useful throughout the entire life cycle of a trade secret; all the way from creation until the potential disclosure.[3] There are mainly two factors causing problems for the trade secret holders; firstly, the complications in establishing proof of ownership, and secondly, the failure to demonstrate reasonable step to keep the trade secret safe. This dissertation will research the possibilities of applying blockchain technology to these two critical factors of trade secret law, with the purpose of enhancing the conditions for trade secret holders to establish and demonstrate compliance with the legal requirements of protection. The aim is to give the reader an informal analysis on how different blockchain technologies, with different initiatives and purposes, can be used to achieve the overall aim of reducing the risk of misappropriation in an ever-evolving digitalised environment. The first section and second section, respectively, (II.) and (III.) will provide the reader with necessary knowledge in the legal landscape of trade secret protection and the use of- and technology behind blockchain. The second section (IV.) will demonstrate the importance of establishing proof of existence for unregistered intellectual property rights. This section will firstly analyse the traditional complications of providing proof of existence, and secondly demonstrate how blockchain technology can help fill this gap. The third section (V.) will explore the legal requirement to demonstrate "reasonable steps" to protect a trade secret and analyse whether the application of blockchain technology, complies with the Trade Secret Directive. After establishing the great potential for the technology to provide trade secret holders with easier measures to demonstrate compliance, section (VI.) will critically assess two of the most emerging issues with implementing blockchain technology to the traditional legal landscape, respectively (VI. 1) the issues with admissibility of blockchain-evidence court proceedings, and (VI. 2) how the General Data Protection Regulation will interact with blockchain technology. The last section (VII.) will provide the conclusion which states an essential need for blockchain-based registers for the purpose of proving proof of existence and reasonable step.

[3] *Birgit Clark, 'Blockchain And IP Law: A Match Made In Crypto Heaven?', WIPO Magazine (2018).*

II. The legal concept of trade secrets

Trade secrets are often seen as a loose concept of law that includes any kind of confidential business information which provides the enterprise with a competitive edge.[4] Trade secrets can therefore exist in an extensive variety of forms, which makes the legal concept very flexible. This can be seen through what has been recognised by the courts as trade secrets, such as source codes, methods, contract terms, business plans, market insights, supplier and customer lists, laboratory notebooks and recipes.[5]

Trade secrets are often seen as a parallel concept to traditional intellectual property rights and can not necessarily be defined as a subset under intellectual property.[6] However, there is a century-old practice of keeping valuable information confidential and the legal concept is today accepted and enforced in most countries equal to traditional intellectual property rights. Trade secret protection has historically been left to the national legislators and therefore also with considerable variations of protections in the different jurisdictions. However, in 2016 the final version of an EU Trade Secret Directive was agreed on and published in the official journal of the European Union. With the Directive is there a clear aim from the legislator to harmonise the legal divergence related to the protection of trade secrets within the EU. The Member States was obliged to implement the directive before 9 June 2018.[7]

Protection through secrecy is often seen as an alternative or substitute to patents protection. The rationale behind patent protection is to provide a legal monopoly for a restricted period of time in exchange for the public disclosure of the invention. The obvious difference between the two legal entities is that for a trade secret you have no monopoly and can thereby risk that the secret gets reviled or simply that another inventor comes up with the same idea and thereby lose all protection. Furthermore, while trade secrets can be held for eternity if kept secret, patents will only be protected for a period of 20 years.[8] Furthermore, there is a fundamental difference in the material scope of protection, where e.g. business methods and software are prohibited from patentability, is the material scope of a trade secret protection almost without borders[9]. The famous Coca Cola formula "merchandise 7X", illustrates some of the advantages of securing

[4] 'What Is A Trade Secret?' (*Wipo.int*, 2019) <https://www.wipo.int/sme/en/ip_business/trade_secrets/trade_secrets.htm> accessed 10/06/2019.
[5] 'The Blockchain For Securing Trade Secrets - Bernstein - Blockchain For Intellectual Property' (*Bernstein*) <https://www.bernstein.io/blockchain-and-trade-secrets> accessed 24/05/2019.
[6] General Court of the EU, case T-167/08, Microsoft Corp. V. Commission, par. 150.
[7] (EU) 2016/943 The Trade Secret Directive.
[8] U.S Patents Act 35 USCS and Convention on the Grant of European Patents.
[9] Article 52 (2) c), European Patent Convention (n.9).

information as a trade secret. Keeping the information as a trade secret made the company able to privately benefit from the information and maintain their competitive advantage for over a century instead of the patents limited monopoly of 20 years.

1. Exponential growth in trade secret litigation

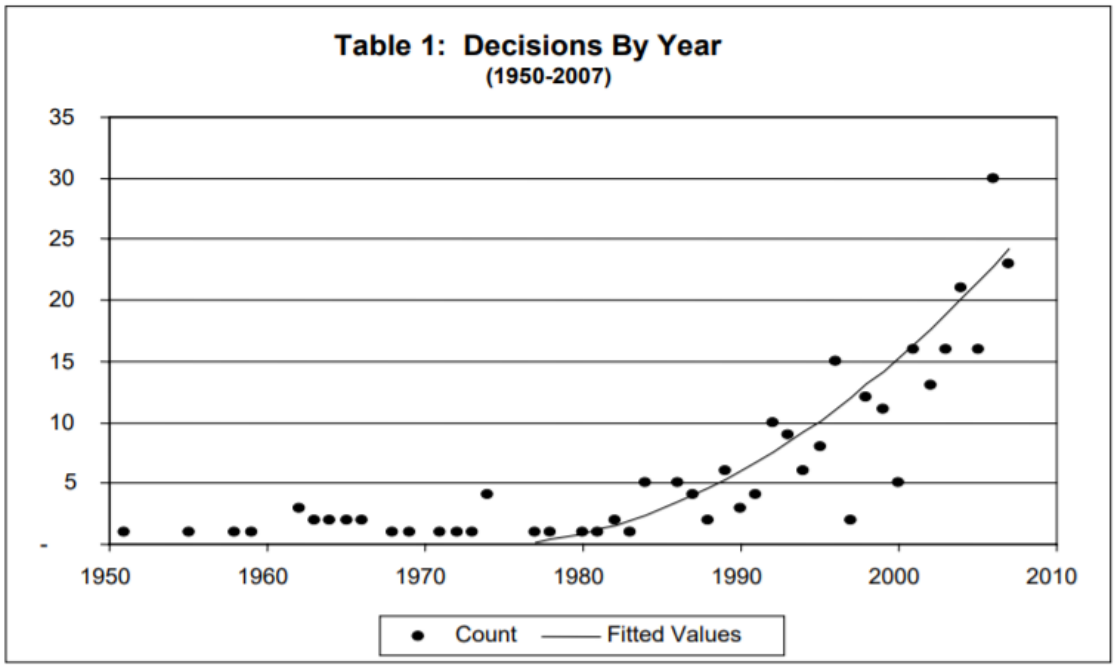

Figure 1:Illustrates the exponential growth of trade secret litigation in the US.[10]

There are mainly two important factors that have contributed to an exponential growth in trade secret litigation in the last decades. Firstly, there has been a massive increase in employee mobility around the turn of the 21st century. Regular job change is becoming a trend, and employees often move to the competitors of their prior employer. There is also a rise in strategic employee poaching by competitors based on the knowledge they can collect.[11] Electronic document storage has also improved massively in the last decade. Digitalisation means that copying and transferring confidential information or knowledge can potentially be as easy as using email- or online file transfer services. This has vastly increased the risk associated with employee mobility.

[10] 5 David S. Almeling et al., 'A Statistical Analysis of Trade Secret Litigation in Federal Courts', *Gonzagla Law Review* v. 45:2 (2010), 302.
[11] Douglas R. Nemec and P. Anthony Sammi, 'The Rise Of Trade Secret Litigation In The Digital Age' (*Skadden*, 2018) <https://www.skadden.com/insights/publications/2018/01/2018-insights/the-rise-of-trade-secret-litigation> accessed 20/05/2019.

These two main considerations are also affected by the accelerating pace of innovation and globalisation that cause the patent system to become less practical and relevant than earlier. With the rising costs and timeliness of patent applications combined with a territorial fragmentised and ineffective environment for patents, trade secret protection is on the rise. This could also be seen through lawmaker's incentive around the globe to updating and harmonising their regulation of trade secrets or confidential information, and at the same time make it easier for trade secret holders to enforce their rights in case of infringement.

Trade secrets have, historically, been secured through physical protection in bank boxes, home safes, and by extensive use of non-disclosure agreements. However, in the modern world with increased digitalisation and employee mobility, as seen in figure 2, about 85 % of all trade secret misappropriation cases concerns theft from employees or business partners.[12] This begs the question if other means such as blockchain-technology can help the trade secret holders to better store their information and enforce and prove misappropriation, and at the same time being lawfully in line with the requirements of the Trade Secret Directive.

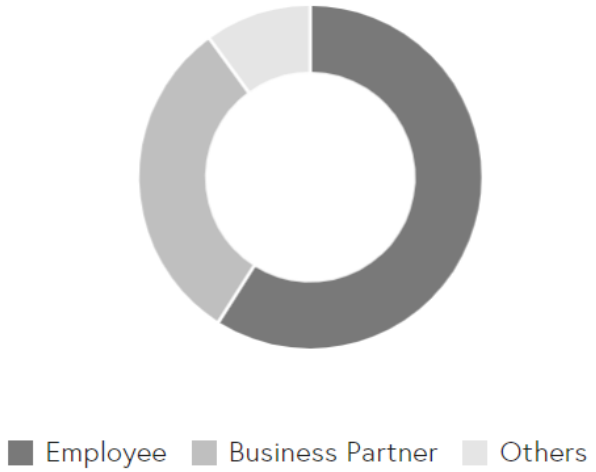

Figure 2: Illustrates the identity of alleged misappropriators of trade secrets <https://www.bernstein.io/blockchain-and-trade-secrets>

III. Blockchain Technology

1. The use cases of Blockchain technology

In order to effectively analyse how and if Blockchain technology can influence and help entrepreneurs secure and enforce their trade secrets, is it necessary to understand what Blockchain is and the relevant detail on how Blockchain technology operates and what it can be used for.

[12] *Supra* note 10, 294.

Blockchain is best known through "Satoshi Nakamoto's" adapted technology that underpinned the cryptocurrency *Bitcoin* and has been a buzzword in the technological world for the last decade. The technology has already begun to revolutionise the finance and banking sector with a digital currency that is not lead by a centralised power but from a peer to peer (P2P) network where the users, based on verification and democratic consensus, secure their own transactions. According to the Harvard Business Review, blockchain is predicted to do to the finance sector what the internet did to traditional media.[13]

It is, however, important to distinguish between the cryptocurrency *Bitcoin* itself and the underlying technology which is Blockchain. It is the technology which persists the real value and has later been extracted from the finance sector and currency exchange, and expanded into several different industries and used for several different purposes.[14] Blockchain has among other, been used to bridge the gap between patients, providers, payers and regulators in the health care sector, and in Estonia 99% of all health data is digitised and blockchain technology is implemented into the system to ensure data integrity and security.[15] The same technology has been used to secure elections and voting-systems where there have long been implications as to the security and democratic legitimacy compared to ordinary elections. This is why blockchain with the help of public ledgers can help run electronic elections with strong security and information flow.[16] Beyond this, blockchain has become a massive resource when it comes to intellectual property rights. Smart contracts connected to blockchain is being used to automatically enforce IP licencing-agreements which allow the transmission of royalties in real time.[17] Kodak is using this technology to store image assets to track ownership rights and licence transactions in order to enforce copyright.[18]

---

[13] 'The Blockchain Will Do To The Financial System What The Internet Did To Media' (*Harvard Business Review*, 2017) <https://hbr.org/2017/03/the-blockchain-will-do-to-banks-and-law-firms-what-the-internet-did-to-media> accessed 15/05/2019.
[14] 'Blockchain Use Cases - IBM Blockchain' <https://www.ibm.com/blockchain/use-cases/> accessed 06/06/2019.
[15] 'E-Health Records — E-Estonia' (*e-Estonia*) <https://e-estonia.com/solutions/healthcare/e-health-record/> accessed 19/05/2019.
[16] John Biggs, 'Sierra Leone Just Ran The First Blockchain-Based Election – Techcrunch' (*TechCrunch*, 2018) <https://techcrunch.com/2018/03/14/sierra-leone-just-ran-the-first-blockchain-based-election/?guccounter=1> accessed 25/05/2019.
[17] Birgit Clark, 'Blockchain And IP Law: A Match Made In Crypto Heaven?' (*Wipo.int*, 2018) <https://www.wipo.int/wipo_magazine/en/2018/01/article_0005.html> accessed 21 May 2019.
[18] 'Kodakone | Image Rights Management Platform' (*Kodakone.com*) <https://www.kodakone.com/> accessed 23/06/2019.

Blockchain-technology has great potential in many industries and is vastly researched and developed for new purposes every day. The main selling-point of Blockchain is that the stored information can be distributed without being accessed, copied, or altered.[19] In the modern age where the balance between security and digitalisation is becoming exponentially harder to fulfil, the security mechanisms of blockchain-technology become increasingly valuable and interesting across every businesses sector and governmental institution.

2. Understanding the technology behind blockchain

A Blockchain in its standard form is a distributed ledger or database of records that are completely open to anyone and shared among participating parties.[20] The Blockchain consists, like the name indicates, of a chain of digital "blocks" where each individual block contains information data and is connected to each other in a chain. Once the information data has been recorded inside the blockchain it becomes practically impossible to alter.[21]

As illustrated in figure 3, each individual block consists of relevant data, depending on what information that is stored (i.e. transactions, health data, or confidential information), a unique fingerprint which identifies each individual block (*a hash*), the hash of the previous block in the chain, and a digital timestamp proving when the data was put into the blockchain.

[19] Aparnaa Balamurali, 'Blockchain Vs. The Law: Can Blockchain And Data Privacy Co-Exist?' (LLM, King's College London 2018).
[20] Michael Crosby and others, 'Blockchain Technology: Beyond Bitcoin' [2016] *Applied Innovation Review* <https://j2-capital.com/wp-content/uploads/2017/11/AIR-2016-Blockchain.pdf> accessed 20/05/2019.
[21] Curtis Miles, 'Blockchain Security: What Keeps Your Transaction Data Safe? - Blockchain Pulse: IBM Blockchain Blog' (*Blockchain Pulse: IBM Blockchain Blog*, 2017) <https://www.ibm.com/blogs/blockchain/2017/12/blockchain-security-what-keeps-your-transaction-data-safe/> accessed 24/05/2019.

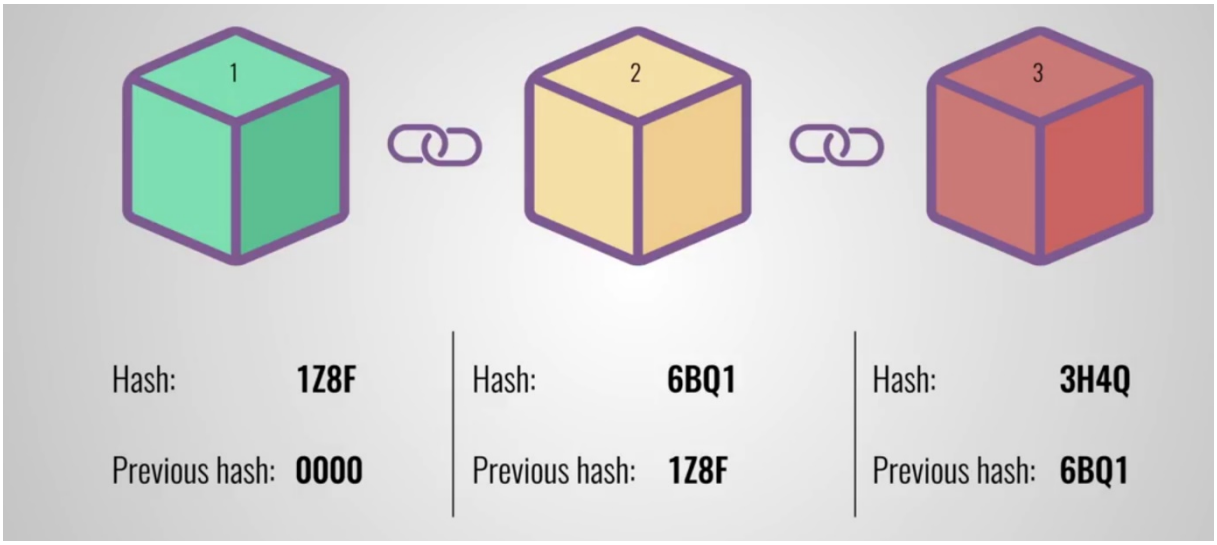

Figure 3: Illustrates how the individual and previous hash connects the blocks together in a chain and constitutes the concept of a blockchain.[22]

If anyone tries to tamper with the data stored on one of the blocks, the hash would change, and the block would no longer be equal to the original. This makes it easy to detect potential alterations in the blockchain as the new block would no longer store a valid hash of the previous block. Furthermore, each individual block consists of the hash of the previous block, making the blocks connected in a chain. This makes it impossible to tamper with only one of the blocks and a potential hacker would have to simultaneously alter a whole chain of blocks to avoid detection.[23]

However, it is not enough to secure the relevant data alone. Because of the massive computing power that exists today, computers can calculate almost infinitely of hash-codes per second and thereby recalculate each hash of the blockchain to validate the chain after it has been tampered with. To mitigate this problem there are further security mechanisms called the consensus mechanism. Because of the decentralised authority of a blockchain network is there no centralised party that makes the decisions. The consensus mechanism constitutes a form of democratic voting process to accept or reject the adding of information to the blockchain and distributed throughout the P2P network. This mechanism makes it almost impossible for third parties to gain access or alter information, as they would have to get consensus from the

[22] Savjee, 'How Does A Blockchain Work - Simply Explained' (*YouTube*, 2017) <https://www.youtube.com/watch?v=SSo_EIwHSd4> accessed 05/05/2019.
[23] Ibid n.23.

network. The influential Silicon Valley entrepreneur Marc Andreessen listed this Blockchain *distributed consensus model* as one of the most important inventions since the internet itself.[24]

3. Public and Private Blockchains

To understand the issues and potential benefit of blockchain technology for securing trade secrets is it also important to understand the difference between a public blockchain and a private or permissioned blockchain.

The main difference between a public and private blockchain relates to who is allowed to participate in the blockchain-network, and thereby also part of the consensus protocol and maintenance of the shared ledger. In a public network, there are no restrictions whereas to who can join, on the contrary, these networks often encourage more people to take part in the blockchain. Unlike for private blockchains, is it almost impossible to identify each individual participant in a public network. The incentive for fairness and good behaviour is therefore not enforced through identity but economics incentives and game theories.[25] Bitcoin is one of the largest public blockchain networks active today.

A private blockchain network is, however, not open to the public and thereby in its core centralised. Every participation requires a personal invitation and must, in addition, be validated from the network starter before gaining access. This is more specifically known as permissioned blockchains. With this blockchain concept, the aim is to control who can write data to the blockchain and at the same time control who can read this data. In order to pursue this aim is it critical that each of the members in the network can be identified and identity management tools are therefore built into the network.[26] When the identity of each individual participant to the network is known, this also means that the network will know exactly who's been misbehaving.

[24] 'Blockchains – "The Most Important Invention Since The Internet Itself"' (*Murfett.com.au*, 2017) <https://www.murfett.com.au/MurfettLegal/media/Documents/Article/35-Blockchains-The-Most-Important-Invention-Since-the-Internet-Itself.pdf> accessed 17/06/2019.
[25] Demiro Massessi, 'Public Vs Private Blockchain In A Nutshell - Coinmonks - Medium' (*Medium*, 2018) <https://medium.com/coinmonks/public-vs-private-blockchain-in-a-nutshell-c9fe284fa39f> accessed 16/06/2019.
[26] Ibid.

IV. Using Blockchain-technology to Comply with the Trade Secret Directive

1. Legal Requirements

Trade secret are in their very nature a "secret" and are protected only as such. This makes the protection of trade secrets a complex area of law that is easily influenced by internal and external circumstances. In an increasingly digitalised world with the widespread use of information technology, worldwide supply chains, and relentless physical and internet exchange of data in every sector of business, is it about time that the trade secret regulations is being harmonised and adapted to the new digital environment and global economy.[27] International, regional and national trade secret laws have shown an increasingly strong focus on what the companies themselves can do, and are obliged to do, to protect their intangible assets. Even though trade secret law in general is governed by national jurisdictions, a general legal protection can be found in Article 39 of the TRIPS agreement, which is also reflected in the new EU Trade Secret Directive.[28] A trade secret, in order to be consider as such, must according to the harmonised definition, meet three accumulative legal requirements; 1) The information cannot be generally known or readily accessible to the people that deal with such information, 2) it must be of commercial value and, 3) the trade secret holder has to take reasonable steps to keep the information secret.[29]

These legal requirements are not only necessary for a trade secret holder to enforce the trade secret, it is on the contrary, a legal requirement for the information to be considered as a trade secret at all, and thereby qualify for protection under the Directive.[30] Failing to fulfil these requirements will preclude a company from getting any legal redress in case of unauthorized disclosure or use of information.[31] The first two requirements, secrecy and commercial value, are technology-neutral and would not cause any new legal or practical issues, despite how or whit what measures information is stored. The interesting question concerns the third requirement, whether the trade secret holder has been subject to "reasonable step" to keep the information secret. This concerns the secret holder's obligations and routines to actively make sure the information stays confidential and is naturally the most disputed requirement in trade secret law. Pragmatically, the complicated part of this last requirement is that the trade secret holder must have three thoughts in mind at the same time. Firstly, make sure that they have solid proof of existence in order to show that they are actually the owner or in control of the

[27] *Supra* note 2.
[28] Article 2, Trade Secret Directive.
[29] Article 39.2 TRIPS.
[30] Article 2(1) c) Trade Secret Directive.
[31] *Supra* note 2.

trade secret. Secondly, the trade secret holder must take reasonable measures to protect the trade secret, so that it will not lose its value by disclosure. Thirdly, in case of misappropriation, is it not enough to have carried out reasonable measures to protect the trade secret, if those measures cannot positively be proven in a court of law. These simultaneous thoughts and compromises are difficult for the trade secret holder to combine.

2. The Problem of Proof of Existence for Unregistered Intellectual Property

For a trade secret holder to have any rights in its trade secret, it must be established that the information in question is rightfully owned and controlled by the claimed trade secret holder. Unlike with patents, where proof of existence and priority date is organized through a formal registry, where the first person to apply for a patent gets the monopoly,[32] trade secret holders are left to themselves when proving the time of creation in order for the court to determine ownership and chronological creation.[33] The burden of proof is therefor put entirely on the trade secret holders themselves.

This automatic protection, that unregistered IP rights benefit from, has often led companies to put their guard down when it comes to establishing proof of existence for their creations.[34] Unlike for registered IP-rights, where active steps must be taken to secure the rights, it is more normal for owners of unregistered IP to limit themselves to act in compliance with "good practice" within a certain jurisdiction, such as established rights through i.e. a bailiff's reports, notarial deposit or through a registered letter proving date of creation. Even though these methods serve its purpose in general, is it clear that they are not designed to keep up with the current developments of trade secrets in the digital world. It is very expensive and ineffective to always make sure your documents are sealed, time-proofed and then physically secured and saved over a longer period of time. Not to mention the complexities in doing this with digital IP assets that can take any technical form. Furthermore, due to the time-consuming nature and lack of focus on proof of existence in unregistered IP, it is common that companies do not

[32] Article 63(1), European Patent Convention.
[33] Alessio Balbo, "Can Blockhain be a "reasonable step" to keep a trade secret safe?
[34] Vincent Fauchoux, Bénédicte Chaniot and William Fauchoux, 'How Can Blockchain Revolutionize The Proof Of Existence Of IP Assets Protected By An Unregistered IP Rights Worldwide?' (*Blockchainyourip.com*, 2018) <https://blockchainyourip.com/wp-content/uploads/2018/12/Blockchain-for-IP-assets-White-Paper.pdf> accessed 21/06/2019, 9.

follow any good practice at all, before realising the importance of proving ownership only just before or in the course of a litigation process.[35]

3. Blockchain And Proof of Existence

At initial view, blockchain-technology has great potential to bridge the gap between the current development in digitalisation of trade secrets and the traditional tools for securing them. The aim is to create a secure, transparent, and more international oriented way of establishing proof of existence.

For companies to benefit from a technical-evoked proof of existence, it is indispensable that the technique used is secure and transparent. If it is not sufficiently protected from cyber-attacks and other digital threats, it is contradicting to register the trade secret for the purpose of proof of existence, only for the information to be disclosed and lose its value. Therefore, the blockchain-network should be built on a decentralised platform. This type of blockchain is, as mentioned, practically immutable, as in order to change the information on one block, a cyber-attacker would have to alter all the blocks in the ledger simultaneously.[36]

This is essentially what makes decentralised blockchains so attractive in the context of establishing proof of existence. A trade secret holder can register a document to the block and establish an electronical timestamp of existence on a trustworthy and transparent record. In order for the information to be verified and registered to the ledger, there must be established consensus between the multiple parties in the network. This process is repeated every time new information is being added to the chain, which means that it is impossible for a single party to later make changes or delete the data already registered. The new blocks of information will always be added to the chain in a chronological order, which makes the whole process transparent. Furthermore, and most crucially, the exchange of information is conducted anonymously, whereby the information is simply translated into a mathematically established hash-code that provides a perfect representation of the information.[37] The trade secret is thereby not publicly available to the network, only in form of a digital symbol of the information,

[35] Ibid.
[36] Birgit Clark and Sylvia Polydor, 'How Blockchain Can Protect Trade Secrets' [2018] Intellectual Property Magazine, 34-35.
[37] Ibid.

namely the hash. In practice, this means that the company will be the only one in possession of an encryption key that can connect the hash-code to the information which is stored behind it.

However, there is never a final truth with digitalisation. An online platform can never be guaranteed to be 100% secure, and the more complex the software, the more vulnerable it is.[38] It bears a great deal of responsibility to the network provider in establishing trust with the users and maintaining and updating security measures. There are several private companies providing proof of existence for trade secret holders using the mentioned technology and methods.[39] This is in fact an easy way of securing proof of existence without engaging in an expensive, time consuming, and political platform involving a governmental or transnational body. WIPO Director General Francis Gurry, is of the opinion that blockchain-technology will revolutionise the traditional function of an IP office when it comes to proof of existence, but "*…will do so by means of a private technology rather than a public register."* [40] This is because the public blockchain-technology establishes independent trust to the public based on its irreversibility and consensus-model with no centralised third party administrating the platform. In theory, this makes it entirely feasible for private companies to provide these services without compromising security. However, this might be a too easy and technological-optimistic view. The fact is that trade secret holders are humans and not only technology-optimists. They would most likely get the chills only thinking about trusting a commercial third party with their trade secrets, singlehandedly to provide a proof of existence, no matter how secure the technology is.

A better solution for generating necessary trust and authority to the service, and at the same time getting the most out of the technology, is to build on EUIPO's feasibility analysis for an EU digital Deposit System ("Feasibility Analysis"), and research the opportunity of developing an IP registry with the help of public institution like EUIPO or WIPO.[41] Unlike private commercial platforms, an EU registry would establish an in-built authority because of its credibility and familiarity with traditional registries of intellectual property rights such as patents registry, trademarks registry, and design registry. Contrarily to these registries, whose purpose is to implement the trade-off between protection and disclosure by publicly disclosing the invention for others to learn from and work around, the purpose of a trade secret registry

[38] E-mail correspondence with Dr Guido Not La Diega (14/08/2019).
[39] See i.e. www.berstein.io
[40] 'Francis Gurry On The Future Of Intellectual Property: Opportunities And Challenges' (*Wipo.int*, 2017) <https://www.wipo.int/wipo_magazine/en/2017/05/article_0001.html> accessed 19/07/2019.
[41] European Union Intellectual Property Office, 'Feasibility Analysis For An EU Digital Deposit System' (EUIPO 2018).

would be to easily prove ownership as well as providing notarization with the help of a digital timestamp on date of creation.[42] A big weakness of the feasibility analysis is, however, that decentralised networks like blockchain did not get considered as platform for the deposit system because it was not yet proved to be an "*established, comprehensive and secure method*".[43] In the authors opinion, this is based on a wrong assumption. It will be demonstrated in the further, how an EU registry for trade secrets can significantly benefit from a blockchain platform.

4. EU Deposit System Built on A Blockchain-Platform

The feasibility analysis proposes two options for a basic deposit system; the EUIPO would either 1) only provide electronic proof of existence with a secured timestamp or, 2) in addition to the first option, also store copies of the content certified.[44] With the implementation of blockchain technology, these options could practically be incorporated into one. The blockchain registry platform would provide a time-stamped proof of existence but only indirectly and anonymously store the relevant content with the EUIPO.[45] To serve its purpose for trade secrets, the registry must be completely confidential, also to the EUIPO, equal to the national IP registries established in Benelux, France and Portugal, and unlike in Italy where the registry is of an administrative public information purpose.[46] The registry would thereby provide a ledger for each individual invention, which would consist of a chain of confidential information, whereas only the hash and timestamp would be public in the registry.

[42] Chagai Vinizky, "Trade Secret Registry", *Pace Law Review* 35:2 (2014), 455.
[43] *European Union Intellectual Property Office, 'Feasibility Analysis For An EU Digital Deposit System' (EUIPO 2018),*
[44] Ibid.
[45] Ibid.
[46] Ibid.

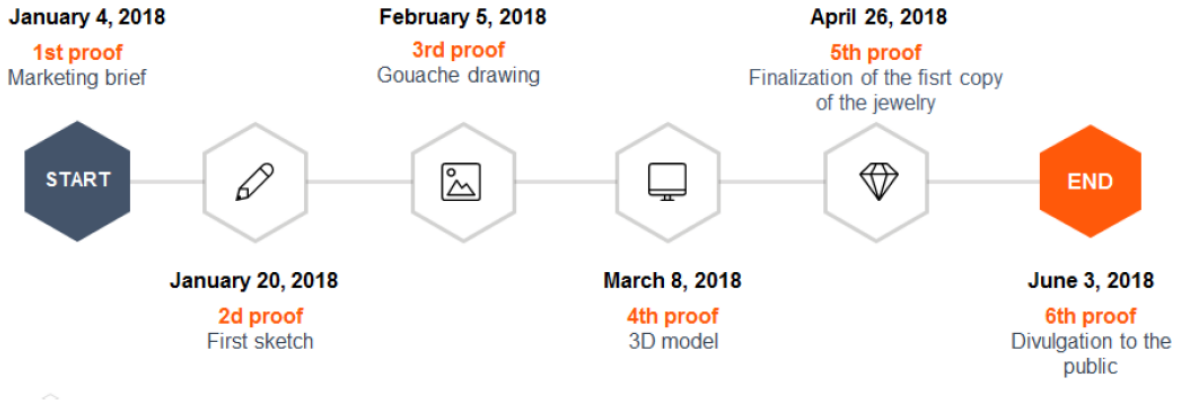

Figure 4: Illustration of every-step registration of a jewellery design.[47]

Figure 4 illustrates how a company, using a blockchain registry, can register all the relevant steps of an invention-process into a ledger, in their path to publicly disclose a jewellery design. Every single step of the process is registered to a specific block in the blockchain, providing an individual hash and timestamp for each block in the ledger. Because of the flexible nature of the blockchain, is it not only possible to register traditional documents, but any format of documents, such as drawings, pictures, 3D models and combination of data and software.[48] This flexibility is absolutely essential for the registry, because a modern trade secret can consist of any physical or electronical format. With a step-by-step registration process stored on a ledger, it is possible for the unregistered trade secret rights to easily establish an immutable, transnational oriented chain of evidence on the whole lifecycle of a trade secret. There is no doubt that this technology could solve the number one issue when it comes to unregistered rights; providing documentation of ownership and existence. Compared to the traditional notarization measures, is it clear that such an authoritative deposit system would drastically reduce time consumption and expenses for enterprises, by providing a simple and inexpensive registry of proof of existence.[49] This is a game-changer for start-ups and small businesses that cannot afford the expenses of traditional security for their IP-assets. Furthermore, in case of misappropriation, there is no longer the need to "dig up" decade-old documents and worry about whether they are time-stamped or not, as the EU blockchain registry will provide a real time chain of proof, which in principle can be put directly before the court as evidence.

[47] *Supre* note 34.
[48] *Supra* note 34.
[49] *Supra* note 43.

The blockchain registry will not only make the process in general more practical and transparent, it will more importantly also build a more secure and trusted alternative for providing proof of existence. The number one trend in cyber-attacks in modern time, is the immense focus on accessing databases that consists of personal data.[50] Yahoo got attacked in 2016 where over 1 billon user accounts got hacked.[51] The same is happening in the public sector where healthcare data is one of the biggest targets.[52] This puts and immense responsibility on the registry platform because of the nature of the data stored. A registry of trade secrets would be of infinite value and would not only be at risk of cyber-attacks, it would be the single most prominent and natural goal for a cyber-crime to take place. The EUIPO concluded after the feasibility analysis that security is "critical" for the implementation of the registry, and that the content managed on behalf of the user must be kept at a "secret" level.[53] This means a security level equal to the *SOC2 standard* of storing data. This is the normal compliance requirement for any company storing costumer data.[54] The biggest issue with the suggested security measures, is clearly that the registry is using a centralised data-platform for providing proof of existence, which allows for one single point of failure. This is not sufficient, as the numerous incidents of cyber-attacks have illustrated the last couple of years. To implement a trade secret registry, it is essential that the platform and database for information-storage is decentralised. Blockchain technology is in its very core designed to have no central authority or data-storage location. This removes the cyber-attackers' single point of entry, because the majority of "nodes" must reach a common consensus, and thereby accept the one trying to access the network. This makes the platform much more secure, as a cyber-attacker would have to hack into every "node" in the network simultaneously to gain access.

When looking at the technological side of the registry, it is important that the blockchain-network is built in a way that satisfies the security measures of a decentralised network, but at the same time gives more control to EUIPO and Member States, than the ordinary public blockchain. This means that the ledger should be distributed on a P2P platform, upholding

[50] 'Cyber Attack Trends Analysis' [2019] *Check Point 2019 Security Report* <http://www.snt.hr/boxcontent/CheckPointSecurityReport2019_vol01.pdf> accessed 10/07/2019.
[51] Vindu Goel and Nicole Perlroth, 'Yahoo Says 1 Billion User Accounts Were Hacked' (*Nytimes.com*, 2016) <https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html> accessed 27/06/2019.
[52] Fred Donovan, 'Healthcare Industry Takes Brunt Of Ransomware Attacks' (*HealthITSecurity*, 2018) <https://healthitsecurity.com/news/healthcare-industry-takes-brunt-of-ransomware-attacks> accessed 06/07/2019.
[53] *Supra* note 43.
[54] Vikram Varakantam, '4 Things You Need To Know About SOC 2 Compliance' (*Threat Stack*, 2018) <https://www.threatstack.com/blog/not-soc-2-compliant-4-reasons-your-customers-wont-work-with-you> accessed 06/08/2019.

necessary security measures, but where the adding of new blocks can only be established by a trusted third party.[55] In such scenario the EUIPO would operate as the trusted third party, but would either way not be able to alter information on previous blocks. The essential importance of trust in the third party, in this model, is what constitutes the biggest problem for private providers. The EUIPO holds a natural trust and authority among the public and is therefore equipped to function as such third party. This is also illustrated through several governments operating as a single centralised trusted party, using blockchain for storing large databases, such as UK for land registers.[56] These registers are not distributed across a P2P network but are entirely centralised, and thereby completely dependent on the trusted party. The combination suggested above would therefore not only benefit from more control through a trusted party but also benefit from the traditional P2P blockchain security measures.

Another option is to build a closed, permissioned distributed ledger blockchain with trusted nodes. This technology is especially explored by banks to use blockchain-platforms to settle payments among themselves.[57] This network sets up a specific number of trusted nodes who each store copies of the blockchain. Since the number of nodes are already defined, the network is able to use the normal mechanisms of consensus when adding to the block. The control over the network is restricted by limiting the permission to store ledgers and add new blocks to a specific number of trusted parties.[58] In such scenario trust in the parties controlling the network is of essential importance, especially when processing trade secrets. Trust is, however, already a factor today, as consumers and citizens are able to trust government agencies or reputable companies with keeping centralised storing of records accurate without any use of blockchain.[59] With such a platform, the best solution would be to use EUIPO as a reference point, so that every Member State in the EU is a functional node, and thereby create a consensus protocol between the EU Member States. This would create a private permissioned internal EU blockchain with total control by the Member States, with enough number of nodes to make the blockchain secure. However, since it still is a private blockchain and the information is not distributed on a P2P network, each individual Member State would have to invest in traditional

[55] Jean Bacon, Johan David Michels, Christopher Millard & Jatinder Singh, 'Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers' *Richmond Journal of Law and Technology no.*1 (2018), 76.
[56] Stan Higgins, "UK Land Registry Plans to Test Blockchain in Digital Push" (2017), <https://www.coindesk.com/uk-land-registry-plans-test-blockchain-digital-push/> accessed 02/04/2019.
[57] *Supra* note 55.
[58] *Supra* note 55.
[59] Izabella Kaminska, "Blockchain's governance paradox", Financial Times (2017), <https://ftalphaville.ft.com/2017/06/14/2190149/blockchains-governance-paradox/> accessed 12/06/2019.

security to protect themselves against potential hackers gaining access to the ledger or taking control over individual nodes.[60]

V. Reasonable Steps to Keep the Trade Secret Safe

After establishing proof of existence, the trade secret holder is also obliged to demonstrate that he has taken reasonable steps to protect the trade secret in question.

There is, unfortunately, no legal definition or preamble that suggests which measures constitute a "reasonable step" in light of the Directive. The term traditionally originates from the TRIPS agreement, but there are several Member States that need to implement this with the Directive. Hence, the new Trade Secret Directive introduces a minimum standard level of protection, and with this, tries to compel and uniform the trade secret legislation across the EU. The harmonisation approach is also affected by the choice of law. Because the law is embodied in a Directive and not a Regulation, it is not directly applicable, but it is rather up to the Member States to devise their own laws to reach the overall goal set out in the Directive. Consequently, the interpretation of what is considered a reasonable step will most likely diverge in the different Member States, especially when it comes to interpreting law up in light of new technological solutions.

Non-withstanding the fact that the Trade Secret Directive in itself is a thorough and important legislative work, none of its provisions mentions how a trade secret should be secured, and therefore leaving it to the discretionary power of the courts to determine whether the trade secret holder has effectively undertaken the obliged and necessary steps in order to keep the information safe.[61] To get the clear and authoritative boundary to this third requirement, there is no other choice but wait until the term crystallises itself through application by national courts and the CJEU, once the directive is implemented by the Member States. Despite this uncertainty, as a general rule, one can already assume that the more controlled the access to and/or use of the secret information has been within a company, the more likely it will be that the information is protected. Furthermore, is it safe to say that there cannot be a single factor of failure or compliance, the issue in question must be considered from a holistically viewpoint where all relevant factors must be considered together. In order to understand the underlying features of the "reasonable step" requirement, it is therefore necessary to analyse the case law

[60] *Supra* note 55.
[61] *Supra* note 34.

in order to learn from the courts who have addressed the issue before. There are few, if any, cases that give general and detailed guidance on what constitutes a reasonable step under the Trade Secret Directive or the TRIPS agreement. The requirement is, however, implemented verbatim or in substantially similar terms in the trade secret regulations of several jurisdictions, most importantly in the US, and establish a general formula of trade secret protection.[62] This means that it is also relevant to look towards other jurisdictions which have adopted the same legal requirement. The aim would be to identify relevant factors and patterns of argumentation emphasised by the courts from a case to case basis, and thereby apply these principles to blockchain technology and analyse whether the use of this technology could comply with the court's argumentation and interpretation.

Some guidance on the interpretation of the new Directive can be found in the civil judgement from the Provincial Court of Madrid regarding disclosure and exploitation of trade secrets.[63] The court found that the steps taken by a trade secret holder to avoid disclosure must be "*adequate and reasonable*", and more importantly, must be conducted both internally and externally. The external step goes directly to the outside threats, while the internal step is meant to limit access to "employees and collaborators" who know or handle confidential information.[64] Regarding the external step to keep a trade secret safe, it is already established from the courts that multiple electronic security measures like traditional encryption, firewalls, and relevant website blockades, in itself would be enough to comply with the requirement.[65] Blockchain-technology, either public or permission-based, would therefore together with traditional encryption and cyber security measures be good enough to comply with the external requirement. Furthermore, there is no requirement that the trade secret holder must *successfully* in keeping the information secret, as long as he demonstrates that reasonable measures to protect it have been taken.[66] However, it is important to note that more than 85% of the trade secret misappropriation cases brought before the US courts, are estimated to involve an internal

[62] *Supra* note 2.
[63] *Civil Judgment No 441/2016, Provincial Court of Madrid, Section 28, Rec 11/2015* (2016).
[64] 'EU Trade Secrets Directive: What Are "Reasonable Steps"? | Lexology' (*Lexology.com*, 2019) <https://www.lexology.com/library/detail.aspx?g=b59572d9-5e29-44e4-b4fe-67c5559bcf32> accessed 03/06/2019.
[65] United States v. Aleynikov, 2011 U.S. Dist. LEXIS 33345, **34 (S.D.N.Y. Mar. 14, 2011), rev'd on other grounds, United States v. Aleynikov, No. 11-1126 (2d Cir. 2012).
[66] Austrian Supreme Court, Decision No 4 Ob 165/16t *of 25 October 2016.*

threat from employees and third parties.[67] Furthermore, it is found that on average, only 3.6% of the total IT budget was spent on securing such internal threats.[68] This shows a clear mismatch between the importance of internal security, and security measures established by the average company.

The analysis of trade secret litigation cases has shown that there are especially three factors that seem to be of essential importance to the courts when it comes to internal security measures; the use of non-disclosure agreements, policies for limiting employee and third party access to the confidential information, and actively making employees and third parties aware that the information in fact is confidential.[69] The importance of these factors in correlation is very well illustrated in the case of *Aetna Inc. v. Fluegel*, where Aetna sought to prevent a former high-level employee to use confidential information in line of his new work for a competing company. The court stated that «*Aetna employees must annually review and agree to nondisclosure requirements. Aetna's high-level employees, including [the defendant], must sign a non-solicitation, confidentiality and nondisclosure agreement. Aetna marks all appropriate documents as confidential and uses technology including password protection and encryption to limit access to confidential information to only key employees*.»[70] These measures were combined more than satisfactory for the court to establish that reasonable steps were taken.

[67] Douglas R. Nemec and P. Anthony Sammi, 'The Rise Of Trade Secret Litigation In The Digital Age' (*Skadden.com*, 2018) <https://www.skadden.com/insights/publications/2018/01/2018-insights/the-rise-of-trade-secret-litigation> accessed 03/06/2019.
[68] Edward Stroz, 'Psychology Is The Key To Detecting Internal Cyberthreats' (*Harvard Business Review*, 2016) <https://hbr.org/2016/09/psychology-is-the-key-to-detecting-internal-cyberthreats> accessed 10/06/2019.
[69] ''Reasonable Measures' For Protecting Trade Secrets: A Primer' (*Winston & Strawn*, 2019) <https://www.winston.com/en/thought-leadership/reasonable-measures-for-protecting-trade-secrets-a-primer.html> accessed 01/08/2019.
[70] Aetna, Inc. v. Fluegel, 2008 Conn. Super. LEXIS 326, *14 (Feb. 7, 2008).

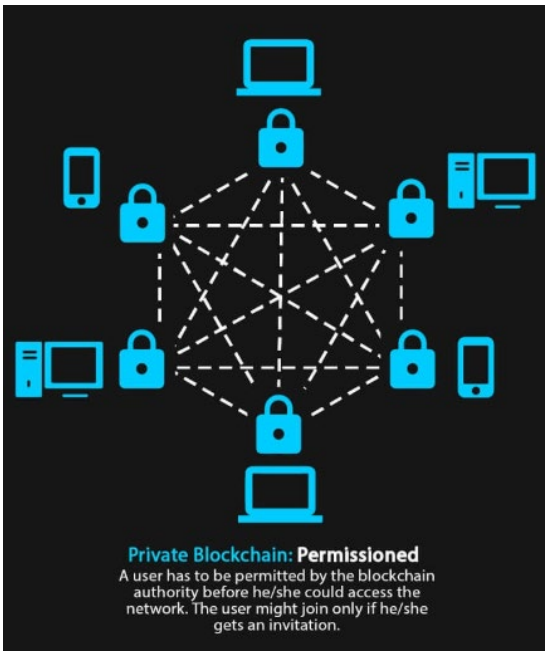

Figure 4: Illustrates a Private Blockchain-network (created by 101blockchains.com)

Many scholars suggest that DLT-technology can be used not only to enhance external security but also to help businesses with their internal security and more easily demonstrate and prove the requirement of reasonable steps. This could be solved by establishing a DLT-network within the business itself, whose aim is to establish control and transparency for the business owners regarding their employees and third parties. With private DLT-technology, the company administration would have to actively permit the individual employee access to the network through establishing a personalised and unique access key which additionally would function as a unique identifier on the individual participant. In accordance with the factors established by the court, the company would control who has had access to what kind of information at any given time, and track when the information was accessed. Furthermore, it is easy for the platform-administrators to explicitly give notice that the information on the block is in fact confidential and not to be shared with others either by communicating that only confidential information is to be stored on the DLT-network or through marking the ledgers. This would make the employee or third party actively aware that the information is confidential, and one would not have to worry about the courts finding a lack of designation putting the employee or third party in doubt on whether he is obliged to keep it secret or not.

At initial view, the private DLT-platform seems to automatically solve most of the legal issues of demonstrating reasonable step - and in theory it does. However, the great potential of private DLT-networks in the context of trade secret protection is somewhat misunderstood. The shadow-side of setting up a private or permissioned blockchain, is that the technology itself can no longer be 100% trusted. The company administration would be able to create consensus internally and thereby singlehandedly possess the power to alter, delete, and add to the blockchain. Even though the company trusts its own DLT-platform and the set-up is perfectly in order and used accordingly, is it always a major issue proving this in court when the whole basis of the platform is relying on trust in the administration running the network. Where there is no longer trust in the technology itself, it is always possible for the legal counterparty to

question the intentions and credibility and use of the platform. This generates the exact same legal implications independent of the implementation of a private DLT-network or not, and makes the platform being near to meaningless for private companies. It is consequently of essential importance in a private blockchain constellation, that the third party administrating the network has a natural authority, credibility and in-built trust with the public. Accordingly, for private companies to benefit from DLT-technology to demonstrate reasonable steps, it is in the authors opinion, an absolute necessity that the DLT-network builds on a public platform, so that the trust is generated by the technology itself and not by the third party running it. This is why private companies instead must dependent on the proof of existence provided through the public Blockchain-network combined with an active NDA to demonstrate the same amount of compliance with the essential factors established in case law, as what was pictured in the "impossible ideal" of a private company-based DLT-platform.

NDA's are often seen as the most important line in defence for trade secret misappropriation and will in some jurisdictions even establish a separate legal basis for protection.[71] A statistical analysis for US trade secret litigation, has found that the courts are almost 25 times more likely to accept that the trade secret holder has established "reasonable steps" with such agreements.[72] However, the biggest problem with the traditional non-disclosure agreement, except from not having one at all, is the requirement to add a definition of the confidential information.[73] These are often drafted either too broad, so that they are not enforceable, or too narrow and specific, so that they instead risk disclosure of the trade secret in question.[74] It is often suggested that DLT-platforms can be used to hold "Smart NDA's" and automatically execute and monitor the contractual codes.[75] The ideal potential here is that the NDA would pop up and automatically demand a signature from each individual employee or third party to gain access to the confidential information. Consequently, the aim would be to track and store the time of access and thereby be able to identify who had access to which information at which time and be certain that the individual has signed an NDA. This is, however, only possible to establish if every participant is uniquely identified through a private key that gives access to a permissioned blockchain. This will again cause the same issues with trust in the platform as the blockchain is controlled by a central authority meaning that time of creation, records of information tracking and time of access can all be altered with, deleted, and added singlehandedly based on

[71] *Supra* note 2.
[72] *Supra* note 10, 301.
[73] *Supra* note 36.
[74] Ibid.
[75] Ibid.

the internal consensus of the company. This does, however, not mean that DLT-technology cannot be of essential importance to establish the requirement of reasonable step. Instead of trying to formulate a bullet-proof NDA that is most likely to be questioned in court, the trade secret holder could link the description directly to the proof of existence. Thus, an NDA will be established, in which the description of the trade secret would not be described by written formulations, but be linked to the certificate of existence of the trade secret, which is established through a hash-code that provides a perfect representation of the information being shared. Since the certificate is established though the public blockchain the network is transparent and open, meaning anyone could access it and check the legitimacy of the hash-code. This direct link between the NDA and the confidential information will make it impossible for the employee or third party to question whether the NDA is enforceable or not. Furthermore, it explicitly proves that the trade secret holder has granted another party access to the trade secret and the use of a hash-code to describe the information, will make the employee or third party actively aware that the information in question is confidential as it is connected directly to the NDA.

Looking at the *Aetna* case and the three main factors for establishing reasonable steps it is clear that the proof of existence established with public DLT-technology together with the use of an active NDA will better the conditions for a company to be able to demonstrate compliance with the Directive.

VI. The Legal Complications Beyond the Trade Secret Directive

When establishing a platform based on the implementation of new technology such as blockchain for the purpose of demonstrating proof of existence and reasonable step, there always is extensive complications in complying with the traditional legal landscape. Two main issues that are of essential interest to analyse further are 1) how traditional courts will accommodate blockchain evidence and, 2) how blockchain will interact with the General Data Protection Regulation (GDPR).

1. The Admissibility of Blockchain-Evidence in Court

a) The Current Status of Blockchain Evidence Before the European Courts

The use of blockchain-based evidence is not something novel in court proceedings in Europe. However, blockchain-evidence has never been guaranteed to be admissible and has only been used through secondary means by hiring expert witnesses explaining what the specific evidence is meant to prove and assuring the court that this evidence is in fact highly legitimate and trustworthy. The problem with treating blockchain evidence as a secondary source, is that the natural authority of the evidence will be impaired and reduced to depend on the judge's knowledge about the technology or the specific expert witness in question. This will also eliminate the potential efficiencies gained using blockchain technology and would instead increase the court costs and decrease access to justice. For trade secret holders this approach will diminish the authenticity of blockchain-evidence and also impair the willingness to invest and rely on the technology. It is therefore essential to analyse if blockchain-evidence could be used as a direct and authoritative source of electronic evidence based on its own legitimacy.

There are no known cases before the European courts that have accepted direct and legally binding evidence based on or created through blockchain technology. National legislators have their own procedural laws on what kind of evidence can be submitted before the courts. This makes the situation somewhat unclear and unpredictable, as considerable variations between the courts in each individual Member State regarding admissibility could arise. Furthermore, as blockchain evidence is not yet approved by none of the EU national courts, there is always a risk that this viewpoint will stay consistent in the future, and thereby deem such evidence not to be legally binding. However, with the implementation of the regulatory framework on "electronical identification and trust services for electronic transactions in the internal market" in 2014, it is no longer possible for EU national courts to deny electronical signatures legal effect.[76] The Framework states that a "*qualified electronic signature shall have the equivalent legal effect of a handwritten signature*".[77] The most important effect of this legislation is that it guarantees uniform application and prevents the courts to reject the data only due to its electronical characteristic. [78]

[76] Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
[77] Article 4(2), ibid.
[78] Jean-Maxime Rivière, 'Blockchain Technology And IP – Investigating Benefits And Acceptance In Governments And Legislations' (2018) 3 Junior Management Science, 10.

b) The Traditional Complications of Electronical Evidence

The traditional concerns about relying on electronical evidence has largely been due to the difficulties in proving its authenticity and integrity.[79] In the modern digital world of electronical evidence, the assessment of authenticity and integrity has to happen constantly throughout the whole chain of existence; all the way from its making to the final submission in court. The main reason for the courts' difficulties in confirming electronical evidence's authenticity and integrity goes to the very core of its characteristics, namely the possibility of digital tampering, and the traditional judges' lack of technological knowledge on the matter.[80] In the same way as an ordinary document provided as proof in court has to be inspected for alterations and forgery, a digital evidence is not different. The problem with digital evidence is the in-built features of easy alteration, forgery or simply that it can be easily deleted by someone with the necessary knowledge. Unlike with tampering physical documents, a regular judge will not possess the necessary knowledge or the professional skill to determine whether the electronical evidence, throughout its whole chain of existence, has been subject to such alterations.

c) Blockchain-Technology Removes the Traditional Concerns in Electronical Evidence

After establishing which factors are critical when it comes to the authenticity and integrity of electronical evidence, it is highly relevant to explore if the same factors can be remedied by blockchain-technology. The main point that distinguishes evidence provided through blockchain from any other electronical evidence, is its character of security and transparency. It is, for all practical purposes, impossible for someone to make alterations, forge, or delete information that is stored on the public blockchain. Consequently, this concerns the first critical factor of electronical evidence, namely security and the risk of evidence-tampering, and thus reduces the risk substantially. This will not only affect the judicial trust and incentive to accept electronical evidence based on blockchain, but it will also affect the second major risk, namely leaving the assessments of technological authenticity to a judge with limited or zero knowledge on the technological structure of the specific evidence in question. When the technology provides for security and transparency in itself, it is no longer necessary for the judges to

[79] David Chaikin, 'Network Investigations of Cyber Attacks: The Limits of Digital Evidence' (2006) 46 Crime, Law and Social Change 239, p. 242.
[80] Reza Montasari, 'Digital Evidence: Disclosure and Admissibility in the United Kingdom Jurisdiction' in Hamid Jahankhani Alex Carlile and others (eds), *Global Security, Safety and Sustainability*(Springer 2017), 45.

investigate whether data has been tampered with and whether there is a difference between the original electronical evidence and a potential duplicated evidence, which is the most difficult problem for traditional methods of identifying electronical evidence.[81] The judiciary will thereby get the opportunity to move its focus and resources away from the impossible task of examining the authenticity and integrity of the electronical evidence's chain of existence, and over to analysing the actual content provided by the evidence. The only crucial point for the judiciary to examine, is whether the submitted electronical document is consistent with the hash-value of the information stored on the blockchain.[82]

d) Blockchain Certifications

Despite blockchain's high level of security, the judicial system can, however, not simply trust that the evidence will be 100% secure and accurate singlehandedly because the evidence is submitted with blockchain. There are many ways to use and build a blockchain network, and the platform is only as secure as its infrastructure. This is frequently demonstrated in this paper with the example of in-house private blockchains that easily can be altered if there is no trusted third party. The court must therefore be observant on who provides the blockchain-platform and how the network is built. The trust in the security and transparency principles of the technology itself, could in the future be confused with blindly trusting the providers and potentially oversee unserious services that build a platform in a way that compromise the very principles that establish the trust in the first place. Therefore, scholars suggest that "new laws of evidence" or "specialist judges" could be a solution to solve the problems with electronic evidence.[83] This was already implemented in China, where they have established specialised internet courts, with specialised judges, designated to consider legal problems that originate from new technologies. However, this requires a considerable transformation of the judicial system, which demands economical investments and governmental administrative measures. This cannot be expected to happen in the near future.

With evidence provided through the means of blockchain technology there is, however, an easier and more realistic solution to minimize the consequences and use of resources for the court when considering the authenticity and integrity in the technology itself. It has already

[81] Hong Wu and Guan Zheng, 'Electronic Evidence In The Blockchain Era: New Rules On Authenticity And Integrity' [2019] SSRN Electronic Journal <https://ssrn.com/abstract=3408896> accessed 06/06/2019.
[82] Ibid.
[83] Kara L Nance, Brian Hay and Matt Bishop, 'Digital Forensics: Defining a Research Agenda', *42nd Hawaii International Conference on System Sciences*(2009), 1-6.

been established how secure and transparent blockchain technology is if the network is built from a serious provider. It is, therefore, natural to move the focus away from the specific consideration of the technology in court proceedings, and rather explore the possibility for the providers themselves to demonstrate compliance with the principles and purpose of the technology. A possible solution is to establish an official grant of certifications to the providers. The certification would tell the world and the court that the blockchain-platform in question is in line with all the necessary security and transparency measures required to create a safe blockchain. This is essential in order to establish trust between the courts and potential private companies providing similar services as the suggested EU trade secret registry. In this way, the providers would benefit from the separation of serious providers from unserious ones, and thereby create trust between the user and the provider. Furthermore, the potential of breach in security because of unserious providers would be considerably reduced. Because the trade secret loses its value when it becomes public, these measures are of essential importance for users to trust third parties with their trade secrets.[84] The suggested certification will additionally reduce the courts doubt in the technology itself, and thereby remove the need for time-consuming authenticity considerations. If the certifications can be trusted, which is a necessity, the judiciaries can finally move away from considering the blockchain-technology as such and perform their traditional function of considering the legal matter in question.

The WIPO and the EUPIO are already actively looking into the capabilities of blockchain, and the potential of developing an official certification should greatly interest them, considering how important blockchain technology will become in the context of intellectual property law in the future.[85] A cooperation between the EUIPO and experts on blockchain technology could easily result in an official certification that establishes a minimum standard of security for third party providers of blockchain networks used in the context of intellectual property. This would generate trust in the technology throughout several jurisdiction at the same time and open for the possibility of operating with an international or EU certification. A similar certification at national level could be generated through governmental agencies. This would generate sufficient trust within the national courts but could be more problematic at international or EU-level, because different jurisdictions could operate with different standards and requirements to achieve such a certification. In any case, it is essential that such a certification comes from a body that generates trust and authority and both considered options would serve this purpose.

[84] Article 2(1), Trade Secret Directive.
[85] *Supra* note 3.

Regarding the suggested EUIPO trade secret registry, the Feasibility Analysis states that it is a prerequisite that the documentation from the registry will be accepted by the EU courts as legally binding.[86] This is only natural if the Member States agrees on establishing such a register, and the courts would thereby be politically imposed to assess such evidence as legally binding. No matter if it is through an EU trade secret registry or establishing official certificates, the EUIPO with its reach and credibility serves an essential role in legitimising the technology and educating the judiciaries on how these evidences can be used before the courts.

e) The International Acceptance of Legally Binding Blockchain-Evidence

Looking beyond the European borders, there is a stronger force towards accepting blockchain-evidence. This could constitute the very start of a legal domino effect, also in Europe.

China has always been eager to be at the forefront of technological developments and adoptions. This is not about to change now, and to state their dominances within innovation and law, China opened the world's first "internet court" in august 2017 in the capital of E-commerce, Hangzhou.[87] As of today, China has also established a second and a third internet court, in Beijing and Guangzhou.[88] The courts have one single purpose; to handle internet related legal disputes. Approximately a year after its opening, a case regarding online copyright infringement was brought before the Hangzhou internet court.[89] The plaintiff captured the violating website and their source code and uploaded the data to a blockchain platform creating an immune record of the copyright infringement. The question on whether blockchain-evidence should be accepted, went all the way to the Chinese Supreme Court. The court stated that *"Internet courts shall recognize digital data that are submitted as evidence if relevant parties collected and stored these data via blockchain with digital signatures, reliable timestamps and hash value verification or via a digital deposition platform, and can prove the authenticity of such technology used*." [90] Thus, the court confirms the tamper-proof nature of blockchain-technology and as long as the source of the network can be confirmed as legit, there is no reason for the

[86] *Supra* note 43.
[87] 'China Focus: China Launches First Internet Court In E-Commerce Hub' (*Xinhuanet.com*, 2017) <http://www.xinhuanet.com/english/2017-08/18/c_136537234.htm> accessed 07/07/2019.
[88] Cao Yin, 'China's Third Internet Court Opens In Guangzhou' (*Chinadaily.com.cn*, 2018) <http://www.chinadaily.com.cn/a/201809/28/WS5badf326a310eff3032801a8.html> accessed 08/07/2019.
[89] Hangzhou Huatai Yimei Culture Media Co., Ltd v Shenzhen Daotong Technology Development Co., Ltd. (Case No.: 055078 (2018) Zhe 0192 No. 81)
[90] The Supreme People's Court of The People's Republic of China, Statement on the admissibility of blockchain evidence [2018] (<http://www.court.gov.cn/zixun-xiangqing-116981.html>)

court to deny direct legal effect of the evidence. The case also illustrates the easy nature of enforcing such evidence in court, as they provide an irreversible timestamp. Furthermore, the Ministry of Investigation Bureau in Taiwan has even launched an app that allows for the judiciaries and legal counterparties to check the authentic of the blockchain evidence only by providing a QR-code.[91]

Even though China is in the very forefront in the development of blockchain evidence, especially the US have established legislation that makes blockchain-evidence admissible. Vermont passed the bill H868 already in 2016 stating that "*A digital record electronically registered in a blockchain shall be self-authenticating*".[92] This was followed by the state of Arizona, passing he Arizona House Bill 2417, stating that "*a signature that is secured through blockchain technology is considered to be in an electronic for and to be an electronic signature*".[93] This is effectively making blockchain-signatures admissible in court proceedings. The latest development occurred in Ohio, they passed the Senate Bill 300, which pretty much mirrors the wording of the two earlier bills.[94] This demonstrates the considerable political motivation and drive force in the US for accepting such evidence in front of the courts. The legal development towards admissibility can accordingly both be established through the courts, like in China, or through political initiative and passing of bills, like in the US.

f) The road ahead

There are several factors that demonstrate why blockchain-based evidence should be admissible before the courts. The traditional concerns regarding electronical provided evidence, is reduced to a minimum with the strict security and transparency features of the public blockchain. This must be seen together with the possibility of regulating private providers through establishing official certifications of blockchain-networks, and thereby create a common trust between the provider, the user, and the court. Based on these facts, there should be no reason for the court to treat blockchain-based evidence any different than the traditionally notary in the form of a physical document. It can already be seen that this point of view is starting to emerge into the

---

[91] 'Taiwan Government'S Initiative To Secure Forensic Evidence With Blockchain' (*Saint-island.com.tw*, 2019) <http://www.saint-island.com.tw/EN/News/News_Info.aspx?IT=News_3&CID=492&ID=1408> accessed 15/08/2019.

[92] An act realting to miscellaneous economic develoments provisions H.868 (Act 157) § 1913(1) Sec. 1.1.12 (2016).

[93] Article 5A, *Aarizona House Bill 2417 on signatures; electronic transactions; blockchain technology (2017)*

[94] 'The Admissibility Of Blockchain As Digital Evidence' (*Concord Law School*, 2019) <https://www.concordlawschool.edu/blog/news/admissibility-blockchain-digital-evidence/> accessed 28/07/2019.

judicial system in several jurisdictions. Having in mind the traditional scepticism towards new technologies and the consecutive slow process of acceptance, it is the compelling that China and US are already in the forefront to accept such evidence. Thus, there is every reason to expect that the "ball will keep rolling" and eventually reach Europe.

To get absolute clarity in the question of admissibility, there is no other option than to wait and see how blockchain-based evidence is accepted across the national courts in the Member States. Nevertheless, some clarity will be established through the EUIPO Observatory's report on litigation trends that must be released before the 9 June 2021.[95]

2. Implications of the new General Data Protection Regulation

The General Data Protection Regulation (GDPR) came into effect on 25 May 2018, and vastly strengthened the EU data protection to meet the new privacy challenges especially brought by the development of new technologies.[96] The regulation has made great impact on every aspect of the law, and companies all over the world which operate towards the European market have been forced to make big amendments to their privacy routines. The many strict rules that came with the regulation, have drawn the question if it is impossible to establish GDPR compliance with new technology like blockchain and if there is place for the regulation and technology to coexist at all. Several scholars support this view, and argue that new technological inventions, which in principle clash with GDPR, must be exempted from the EU data protection regulation for the technology to be able to grow, innovate and serve its purpose.[97] However, this point of view is simply built on a wrong assumption on the dynamics between the GDPR and technology. GDPR compliance is not about the technology as such, it is about how the technology is being used.[98] It is important to understand that there is no such thing as GDPR compliant internet, AI, or blockchain, only GDPR compliant use cases and applications.[99] To consider the implications of the GDPR on blockchain technology, it is therefore necessary to analyse the interplay between these two opposites on a case to case basis.

---

[95] Article 18, Trade Secret Directive.
[96] Regulation (EU) 2016/679, General Data Protection Regulation.
[97] Shannon Liao, 'Major Blockchain group say Europe should exempt Bitcoin from new data privacy rule' (The Verge, 5 July 2018) <https://www.theverge.com/2018/4/5/17199210/blockchain-coincenter-gdpr-europe-bitcoin-data-privacy>.
[98] The European Union Blockchain Observatory and Forum, 'Blockchain And The GDPR' (*Eublockchainforum.eu*, 2018) <https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf> accessed 8/06/2019.
[99] Ibid. 6.

Blockchain-technology is, as mentioned, built on a foundation of immutability, where the very point of its existence is to create an irreversible and incorruptible ledger to secure information. The main purpose of the technology is therefore to make it as hard as possible to tamper with or delete the information which is stored on the chain. On the other hand, GDPR is a legislation, whose purpose is to give control back to the individual over his or her personal data. This is done through establishing extensive rights for the individual to control the maintenance of their personal data, with the threat of heavy fines for the controllers.[100] There is no doubt that there is a general clash of function between blockchain's irreversibility and the GDPR's extensive assumption that all data can be modified or erased to comply with privacy principles. The interesting thing, however, is that even though there is a functional clash in general, there is also a common ideological ground; the aim to protect data. Both the GDPR and blockchain-technology are seeking to increase security in the sphere of data collection. The GDPR accomplishes this by holding the controller, processors and sub-processors of data to a high legal standard, while blockchain with its encryption and decentralized structure makes the data-network highly tamper-resistant.[101] The very same goes for the principle of transparency. The GDPR introduced a new standard of transparency, where the individual has statutory rights to get informed about what is stored, right to access, and right to control this data.[102] With blockchain the principle of transparency goes to the very core of the technology. The technology is made in a way that offers clear and direct access to the data, and the whole history of the chain is available at any point.

With the acknowledgement that the two concepts clash in function but in the end have the same ideological common ground, it should be possible to find a way to combine the two, and find a use of blockchain that is compliant with the GDPR. There are several potential issues regarding GDPR and Blockchain, however, the material scope of the regulation and the individual's right to rectification and erasure of personal data have arisen as the most relevant discussion points.

[100] Article 83, GDPR.
[101] Darryn Pollock, 'How Can Blockchain Thrive In The Face Of European GDPR Blockade?' (*Forbes.com*, 2018) <https://www.forbes.com/sites/darrynpollock/2018/10/03/how-can-blockchain-thrive-in-the-face-of-european-gdpr-blockade/#1201ac0c61df> accessed 22/07/2019.
[102] Article 12-15, GDPR.

a) Material Scope of the Regulation

The material scope of the GDPR applies to "personal data".[103] This is defined as "*any information relating to an identified or identifiable natural person*".[104] Data that is not identifiable or related to a natural person is accordingly outside the material scope of the GDPR. The same goes for information regarding legal persons.[105] Most trade secrets are related to inventions and would thereby consist of technical or business-related information that have nothing to do with a natural person. The issues with blockchain's irreversibility in light of the GDPR would therefore not be an issue with the traditional trade secrets that do not consist of personal data.

However, the scope of personal data is interpreted very broadly by the courts, and has led scholars to argue that data protection has raised to become "the law of everything" as we are rapidly moving towards a future where all data can be subject to some kind of personal data.[106] This is illustrated in the *Nowak case,* where the court explicitly stated that *"the aim of the EU legislature [is] to assign a wide scope to [personal data]*."[107] This means that the potential for trade secrets to include some form of personal information is prominent, because a trade secret in theory can consist of any information, including names, addresses, client lists etc. This would clearly fall under the scope of the GDPR and the individual rights to erasure and rectification would apply.

However, the GDPR only applies to what is "identifiable" to a natural person. This means that GDPR is not applicable where the data in question is anonymised.[108] The threshold for what can be qualified as being anonymised data is however, set very high. Firstly, the technique of anonymisation must make it impossible to identify the natural person through all the "*means reasonably likely to be used*".[109] Secondly, the anonymisation-technique that is used must be irreversible, so that it is impossible to reconcile the original data.[110] This means that personal data even includes pseudonymised data, meaning that the data has been processed such as it

[103] Article 1, GDPR
[104] Article 4(1), GDPR
[105] Bart van der Sloot B, 'Do Privacy and Data Protection Rules Apply to Legal Persons and Should They? A Proposal for a Two-Tiered System', 31 Computer Law and Security Review (2015).
[106] Nadezhda Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law', *Law, Innovation and Technology 10:1* (2018), 40.
[107] *Nowak* C-434/16 [2017] EU:C:2017:994, 34.
[108] Article 4(1), GDPR.
[109] Recital 26, GDPR.
[110] Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques (WP 216) 0829/14/EN.

"can no longer be attributed to a specific data subject without the use of additional data", and is consequently not irreversible.[111] This is also illustrated in *Digital rights Ireland,* where the court held that metadata, which is data that provides data about other data, *may* allow for indirect identification of a data subjects, and thereby qualifies as personal data.[112]

An often-mentioned technique that commentators argue should fulfil the requirements of anonymisation when using blockchain is encryption or hashing. Following the Working Party's opinion on cloud computing, it is clear that encryption of the personal data alone "*may significantly contribute to the confidentiality of personal data if implemented correctly*", however it does not "*render personal data irreversibly anonymous*."[113] The same is said for the use of hash functions, where the data is hidden behind a mathematical function that is transformed into an output value or fixed length.[114] These two technical measures to hide the identity of the data subject would only result in pseudonymisation. Commentators have argued that a combination of these and additional anonymisations measures like "salting" and "peppering" which includes adding information to make it large enough that it is extremely unlikely for someone to reverse the data.[115] However encryptions, hashing and additional anonymisation measures would only account in the adding of measures that are already specifically classified as only pseudonymisation measures alone. This high threshold in a digital environment makes it almost impossible to rely on anonymisation to go clear of the jurisdiction of GDPR when using blockchain to process personal data. Consequently, the administrator would most likely have to build a blockchain network and process the data in a matter that would comply with the GDPR. This is further discussed below.

b) The individual rights of the data subject

To strengthen the data subject's control over their own data is the GDPR introducing several new rights for the individual. Two of the most important rights for the data subject is the right

[111] Article 4(5), GDPR.
[112] *Digital Rights Irland* C-293/12 and C-594/12 [2014] EU:C:2014:238.
[113] Article 29 Working Party, Opinion 05/2012 on Cloud Computing (WP 196) 01037/12/EN.
[114] Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques (WP 216) 0829/14/EN, 20.
[115] *Supra* note 98, 22.

to rectification[116] and the right to be forgotten.[117] These rights can both be at risk of being violated when implementing the use of blockchain for trade secret.

The right to rectification is a consequence of the principle of data accuracy and the purpose is for the data subject to be able to object and correct inaccurate personal data or make supplementary statements so that personal data which is incomplete can become complete.[118] The "right to be forgotten" is a consequence of the principle of data minimization and provides the data subject with the right to demand erasure of the personal data stored about them, if certain requirements are met.[119] As already mentioned, the concept of blockchain technology is to design a network that makes sure that once data is established to the chain, is it impossible to change. The immutability of the technology is the key concept of blockchain.[120] This begs the question how the data subject is able to exercise the right to erasure or rectification when the purpose with blockchain is to make sure this does not happen?

aa) Right to Rectification

According to Article 16 GDPR the data subject has the right to obtain the rectification of inaccurate personal data concerning him or her. For private or permissioned blockchain-networks is it technically possible to create a set-up that based on consensus in the network can support a request of rectification through alteration of the relevant ledger by re-hashing the blocks that provide inaccurate information.[121] This is a helpful solution for internal blockchain networks, where the access point is led by the company itself. However, this also proves the already mentioned core issue with permissioned blockchains administered internally by private companies. The third party does not possess a natural acceptance from the society which generates trust in the accuracy of the alterations to the blockchain. Furthermore, the same concept is very hard to implement for public blockchain networks as every node must personally be altered and accepted from the common consensus in line with each rectification request.[122] However, GDPR provides for an alternative way of implementing rectification; by the means of "providing a supplementary statement".[123] This can easily be solved through

[116] Article 16, GDPR.
[117] Article 17, GDPR.
[118] Article 16, GDPR.
[119] Article 17, GDPR.
[120] *Supra* note 98, 25.
[121] *Supra* note 55, 76.
[122] Panel for the Future of Science and Technology (European Parliment), "Blockchain and the General Data Regulation: Can distributed ledgers be square with European data protection law" (2019), 73.
[123] Article 16, GDPR.

adding a new block to the ledger and refer to the inaccurate information in the earlier block, and thereby provide the new and corrected information. Some argue that supplementary statements might not be sufficient in all circumstances for rectifying inaccurate information. This is implied in the *Nowak case* by the Advocate General Kokott, who stated that the right to rectification has to be *"judged by reference to the purpose for which the data was collected and processed".*[124] However, as long as supplementary statement is clear and precise in its form and reference, and makes it unquestionable that the statement in fact is correcting the inaccurate information in the earlier block, there is no reason why this should not comply with the rational in Article 16 GDPR. If the information is fundamentally wrong and of essential importance, the data subject could always claim for the information to be erased based on the legal grounds in Article 17 GDPR. If there is no legal ground for erasure, this should be reason enough to argue that the mere provision of a supplementary statement ought to be considered sufficient.

bb) Right to Erasure

In the wake of *Google v Spain,* the "right to be forgotten" was implemented as a new right for the data subject with GDPR.[125] According to Article 17 GDPR the data subject has "the right to obtain the erasure of personal date concerning him or her" on certain grounds stated in a) – f). Trying to delete data from the blockchain is purposely made incredibly hard because of the fundamental design of irreversibility. In order to technically be able to delete a block in a blockchain ledger, the whole network of nodes, through the consensus-mechanism would have to verify every single effected block backwards, unbuild the whole blockchain block for block and then rebuild it afterwards, with every step of the way to be distributed block-wise to all existing nods.[126] This might be technical feasible in theory, especially in permissioned blockchain network within a company where it is easier to collectively change the blocks and verify the rebuild. However for the suggested European registry, with potentially thousands of demands of erasure from individuals all over Europe, is it not practical or sustainable that every individual node in the network would have to erase the block in question and thereby rebuild the whole ledger for each request put forward. For a platform powered by public blockchains it is for all practical purposes impossible to delete data by request.

[124] Opinion of AG Kokott in Case C-434/16 *Peter Nowak* [2017] EU:C:2017:582, para 35.
[125] Case C-131/12 *Google Spain [2014] EU: EU:C:2014:317.*
[126] Matthias Berberich and Malgorzata Steiner, 'Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers?', European Data Protection Law Review v.2 (2016), 422-426.

It can however be argued that the right to be forgotten is not an absolute right. The GDPR permits the data controllers to "*take account of available technology and the cost of implementation*".[127] It can therefore be argued that GDPR opens for technological solutions, such as blockchain, that has an inherent difficulty in enhancing the right to be forgotten in the traditional way. This must be seen in context with the term "erasure" which remains unclear as to whether the data ought to be positively destructed for the requirement to be fulfilled. Both the Working Party opinion and the Australian Data Protection Authority are indicating that there may be more than one interpretation of erasure, where respectively the destruction of hardware and anonymisation could qualify as erasure.[128]

In the CJEU there are two contradicting indications on how to interpret the term "erasure". In *Google Spain* the simple measure of de-listing information from Google's search engine was considered sufficient to qualify as erasure.[129] The court's interpretation clearly points in the direction that erasure in the eyes of the regulation can be achieved by other means than the actual destruction of information. On the other hand, in the *Nowak* case the court stated that "*the right to ask the data controller to ensure that his examination answers and the examiner's comments with respect to them are, after a certain period of time, erased, that is to say, destroyed».*[130] Even though the case was not directly dealing with the right to be forgotten, the statement is, unlike in Google Spain, clearly indicating that erasure equals destruction of data. When analysing these two contradicting cases, there is however a huge difference in complexity on how to erase the data in question. In the *Nowak case* the easiest and most straight forward alternative for erasure was for the controller to just destruct the exam paper. In such a case there is no need to even consider other options in light of "available technology". In the *Google Spain* case, which considered data stored on the internet, it was naturally much harder for the controller to destruct the data, and the court accepted that the technological measure of de-listing was considered sufficient. Consequently, it seems like there are more than one alternative for erasure of data, and that the court are more lenient and flexible as to the term "erasure" when considering the technological and practical difficulties of actual destruction.

---

[127] Aricle 17(2), GDPR.
[128] Article 29 Working Party, Opinion 05/2012 on Cloud Computing (WP 196) 01037/12/EN, 12. & Austrian Data Protection Authority, DSB-D123.270/0009-DSB/2018 (2018) <https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181205_DSB_D123_270_0009_DSB_2018_00/DSBT_20181205_DSB _D123_270_0009_DSB_2018_00.html.>
[129] Supra note 125.
[130] 2 Case C-434/16 Peter Nowak [2017] EU:C:2017:994, para 52.

When looking at efficient technical solutions on complying with the right to be forgotten for blockchain technology, the single most mention solution is the option of destructing the private access key.[131] This would have the effect to limit or disable access to the data in question by either using a private key to only applicable for the data subject, or encrypt the private access key so no not even the data subject could access the data that is up for erasure.[132] This is the solution put forward from the French Data Protection Authority in its recommendation on blockchain in the GDPR era.[133] Such a technique of "deleting" the access-point to the information can easily be established in the in-house permissioned blockchain by simply withdrawing everyone's, or everyone but the data subject's private key of access to the information in question. In the suggested EU registry, the public keyed hash function's secret key would have to be deleted together with the information from other systems where it was stored for processing.[134] Here that would be most likely be of the countries using the registry within the European Union.

Considering the above, blockchain-technology are neither GDPR compliant nor not compliant in general. It all depends on which blockchain is used, what information is stored and what technical measures of erasure are available. Either way the GDPR can be and must be a flexible framework to allow technologies like Blockchain to work towards the same common aim; to protect data.

[131] *Supra* note 122.
[132] Giuseppe Ateniese, 'Redactable Blockchain – or – Rewriting History in Bitcoin and Friends' (2017 IEEE European Symposium on Security and Privacy (EuroS&P).
[133] Commission Nationale Informatique et Libertés, 'Premiers Éléments D'Analyse De La CNIL: Blockchain' (2018), 8-9.
[134] Ibid.

VII. Conclusion

The only thing that can fight technology is new technology.

The analysis of the legal situation on trade secret protection as of today, demonstrates a historically underprioritized legal system which uses has, in line with technological growth, expanded exponentially. This has put pressure on the legislators, which resulted in a harmonisation of the legal framework with the Trade Secret Directive. However, the core character of secrecy in light of the immense urge of digitalisation, makes it considerably harder for a trade secret holder to demonstrate compliance with the legal requirements. The traditional means of protecting trade secrets are no longer relevant, as trade secret holders are exposed to new digital threats today in comparison of those of a couple of decades ago. Due to the massive increase in employee mobility and use of digital data storage, it has become much easier to conduct internal trade secret thefts, which skyrocketed misappropriation litigation. As demonstrated above, there are two main factors in the trade secret law that often cause loss for the trade secret holder. Namely, the failure of demonstrating a time of creation throughout a secured and trusted proof of existence, and the failure to demonstrate reasonable steps to keep the trade secret safe.

This dissertation has provided an informal analysis on how blockchain technology can be used to alleviate the downsides of digitalisation and help trade secret holders establish compliance with the legal requirements and demonstrate this in case of misappropriation. This has been demonstrated through suggesting a blockchain-based system for proof of existence. The suggested EUIPO Blockchain registry would create an irreversible and secured proof of existence, which can establish a timestamp on each individual step of the innovation process. The credibility and trust in the EUIPO would implement such a registry with great legal force and provide the judiciaries with necessary trust in the provider. Furthermore, linking the individual description of the invention in the NDA to an irreversible hash-code provided by a blockchain registry, removes any objections on the enforcement of the NDA and simultaneously establish an immediate and clear sphere of secrecy. Nevertheless, EUIPO's credibility and trust can also rub off on private commercial providers through the establishment of a blockchain providers-certificate. This would create both trust with the user and with the courts. However, the legal framework of the GDPR must always be considered when creating both the blockchain-platform and when considering what information can be registered to the network. As long as this is seriously considered is it only a myth that blockchain in itself cannot be GDPR-compliant.

Even though there are great uncertainties in the admissibility of blockchain evidence before the European Courts, the analysis has shown that the traditional authenticity and integrity issues of the traditional electronical evidence is reduced to a minimal with blockchain technology. China and the US are already accepting these evidences as legally binding, and there should be no reason for the European courts to turn another direction.

There is no doubt that Blockchain-based platforms for the purpose of securing trade secrets are here to stay, and most importantly revolutionise the proof of existence, as long as the many pitfalls spelled out in this dissertation are taken into account.

Bibliography

Legislation

Arizona House Bill 2417 on signatures; electronic transactions; blockchain technology (2017)

Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994 (TRIPS Agreement).

An act realting to miscellaneous economic develoments provisions H.868 (Act 157) § 1913(1) Sec. 1.1. 12 (2016).

Convention on the Grant of European Patents of 5 October 1973.

Defend Trade Secrets Act of 2016 (DTSA) (Pub.L. 114–153, 130 Stat. 376, enacted May 11, 2016, codified at 18 U.S.C. § 1836, et seq.

Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

Ohio Senate Bill 300 to amend sections 1306.01, 1306.04, and 1306.06 of the Revised Code to amend the Uniform Electronic Transactions Act to define records and contracts secured by blockchain technology as electronic records and to allow the use of smart contract terms (2017-2018).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

United States Code: Patents, 35 U.S.C. §§ 31-114 (1946) (U.S Patents Act 35 USCS)

Cases

Aetna, Inc. v. Fluegel, No. 074033345S, 2008 Conn. Super. LEXIS 326 (Conn. Super. Ct. Feb. 7, 2008).

Austrian Supreme Court, Decision No 4 Ob 165/16t of 25 October 2016.

Civil Judgment No 441/2016, Provincial Court of Madrid, Section 28, Rec 11/2015 of 19 December 2016

Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others Cases C-293/12 and C-594/12 [2014] EU:C:2014:238.

Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González Case C-131/12 [2014] EU:C:2014:317.

Hangzhou Huatai Yimei Culture Media Co., Ltd v Shenzhen Daotong Technology Development Co., Ltd. (Case No.: 055078 (2018) Zhe 0192 No. 81)

Opinion of Attorney General Kokott in Case C-434/16 Peter Nowak [2017] EU:C:2017:582.

Peter Nowak v Data Protection Commissioner Case C-434/16 [2017] EU:C:2017:994.

The Supreme People's Court of The People's Republic of China, Statement on the admissibility of blockchain evidence [2018] (<http://www.court.gov.cn/zixun-xiangqing-116981.html>)

*United States v. Aleynikov, 2011 U.S. Dist. LEXIS 33345, **34 (S.D.N.Y. Mar. 14, 2011), rev'd on other grounds, United States v. Aleynikov, No. 11-1126 (2d Cir. 2012).*

Official Rapports

Article 29 Working Party, Opinion 05/2012 on Cloud Computing (WP 196) 01037/12/EN.

Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques (WP 216) 0829/14/EN.

Commission Nationale Informatique et Libertés, 'Premiers Éléments D'Analyse De La CNIL: Blockchain' (2018).

European Union Intellectual Property Office, 'Feasibility Analysis For An EU Digital Deposit System' (EUIPO 2018).

Panel for the Future of Science and Technology (European Parliment), "Blockchain and the General Data Regulation: Can distributed ledgers be square with European data protection law" (2019).

The European Union Blockchain Observatory and Forum, 'Blockchain And The GDPR' (Eublockchainforum.eu, 2018) <https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf> accessed 8 June 2019.

Articles

David S. Almeling et al., 'A Statistical Analysis of Trade Secret Litigation in Federal Courts', Gonzagla Law Review v. 45:2 (2010), 301.

Alessio Balbo, "Can Blockhain be a "reasonable step" to keep a trade secret safe?

Bart van der Sloot B, 'Do Privacy and Data Protection Rules Apply to Legal Persons and Should They? A Proposal for a Two-Tiered System', 31 Computer Law and Security Review (2015)

Beth Z Shaw, 'Judging Juries: Evaluating Renewed Proposals for Specialized Juries from a Public Choice Perspective' (2006) 10 UCLA Journal of Law and Technology 3.

Birgit Clark and Sylvia Polydor, 'How Blockchain Can Protect Trade Secrets' [2018] Intellectual Property Magazine, 34-35.

Birgit Clark, 'Blockchain And IP Law: A Match Made In Crypto Heaven?', WIPO Magazine (2018).

Chagai Vinizky, "Trade Secret Registry", Pace Law Review 35:2 (2014).

David Chaikin, 'Network Investigations of Cyber Attacks: The Limits of Digital Evidence' (2006) 46 Crime, Law and Social Change 293.

Giuseppe Ateniese, 'Redactable Blockchain – or – Rewriting History in Bitcoin and Friends' (2017 IEEE European Symposium on Security and Privacy (EuroS&P)

Jean Bacon, Johan David Michels, Christopher Millard & Jatinder Singh, 'Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers' Richmond Journal of Law and Technology no.1 (2018), 76.

Jean-Maxime Rivière, 'Blockchain Technology And IP – Investigating Benefits And Acceptance In Governments And Legislations' (2018) 3 Junior Management Science.

Kara L Nance, Brian Hay and Matt Bishop, 'Digital Forensics: Defining a Research Agenda', 42nd Hawaii International Conference on System Sciences (2009).

Matthias Berberich and Malgorzata Steiner, 'Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers?', European Data Protection Law Review v.2 (2016), 422-426.

Nadezhda Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law', Law, Innovation and Technology 10:1 (2018)

Ray Kurzweil, 'The Law of Accelerating Returns' (2001).

Reza Montasari, 'Digital Evidence: Disclosure and Admissibility in the United Kingdom Jurisdiction' in Hamid Jahankhani Alex Carlile and others (eds), Global Security, Safety and Sustainability (Springer 2017).

Miscellaneous

'China Focus: China Launches First Internet Court In E-Commerce Hub' (Xinhuanet.com, 2017) <http://www.xinhuanet.com/english/2017-08/18/c_136537234.htm> accessed 7 July 2019.

'China Focus: China Launches First Internet Court In E-Commerce Hub' (Xinhuanet.com, 2017) <http://www.xinhuanet.com/english/2017-08/18/c_136537234.htm> accessed 7 July 2019.

'Cyber Attack Trends Analysis' [2019] Check Point 2019 Security Report <http://www.snt.hr/boxcontent/CheckPointSecurityReport2019_vol01.pdf> accessed 10 July 2019.

'EU Trade Secrets Directive: What Are "Reasonable Steps"? | Lexology' (Lexology.com, 2019) <https://www.lexology.com/library/detail.aspx?g=b59572d9-5e29-44e4-b4fe-67c5559bcf32> accessed 3 June 2019.

'Exponential-Growth Dictionary Definition' (Yourdictionary.com, 2019).

'Francis Gurry On The Future Of Intellectual Property: Opportunities And Challenges' (Wipo.int, 2017) <https://www.wipo.int/wipo_magazine/en/2017/05/article_0001.html> accessed 19 July 2019

'Reasonable Measures' For Protecting Trade Secrets: A Primer' (Winston & Strawn, 2019) <https://www.winston.com/en/thought-leadership/reasonable-measures-for-protecting-trade-secrets-a-primer.html> accessed 1 August 2019

'Taiwan Government's Initiative To Secure Forensic Evidence With Blockchain' (Saint-island.com.tw, 2019) <http://www.saint-island.com.tw/EN/News/News_Info.aspx?IT=News_3&CID=492&ID=1408> accessed 15 August 2019.

'The Admissibility Of Blockchain As Digital Evidence' (Concord Law School, 2019) <https://www.concordlawschool.edu/blog/news/admissibility-blockchain-digital-evidence/> accessed 28 July 2019.

'Reasonable Steps' To Protect Trade Secrets: Leading Practices In An Evolving Legal Landscape' (Create.org, 2015)<https://accounsel.com/wpontent/uploads/CREATe_org_Trade_Secrets_Reasonable_Steps_7_15_15_Final.pdf> accessed 4 July 2019.

Austrian Data Protection Authority, DSB-D123.270/0009-DSB/2018 (2018) <https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181205_DSB_D123_270_0009_DSB_2018_00/DSBT_20181205_DSB _D123_270_0009_DSB_2018_00.html.>

Cao Yin, 'China's Third Internet Court Opens In Guangzhou' (Chinadaily.com.cn, 2018) <http://www.chinadaily.com.cn/a/201809/28/WS5badf326a310eff3032801a8.html> accessed 8 July 2019.

Darryn Pollock, 'How Can Blockchain Thrive In The Face Of European GDPR Blockade?' (Forbes.com, 2018) <https://www.forbes.com/sites/darrynpollock/2018/10/03/how-can-blockchain-thrive-in-the-face-of-european-gdpr-blockade/#1201ac0c61df> accessed 22 July 2019.

Fred Donovan, 'Healthcare Industry Takes Brunt Of Ransomware Attacks' (HealthITSecurity, 2018) <https://healthitsecurity.com/news/healthcare-industry-takes-brunt-of-ransomware-attacks> accessed 6 July 2019.

Hong Wu and Guan Zheng, 'Electronic Evidence In The Blockchain Era: New Rules On Authenticity And Integrity' [2019] SSRN Electronic Journal <https://ssrn.com/abstract=3408896> accessed 6 June 2019.

Izabella Kaminska, "Blockchain's governance paradox", Financial Times (2017), <https://ftalphaville.ft.com/2017/06/14/2190149/blockchains-governance-paradox/> accessed 12 June 2019.

Mani VS Sancheti, 'Economic Approaches To Remedies In Trade Secrets Cases' (Cornerstone.com, 2016) <http://www.cornerstone.com/Publications/Articles/Economic-Approaches-to-Remedies-in-Trade-Secrets-Cases> accessed 9 May 2019

Nemec DP Sammi, 'The Rise Of Trade Secret Litigation In The Digital Age' (Skadden.com, 2018) <https://www.skadden.com/insights/publications/2018/01/2018-insights/the-rise-of-trade-secret-litigation> accessed 3 June 2019.

Shannon Liao, 'Major Blockchain group say Europe should exempt Bitcoin from new data privacy rule' (The Verge, 5 July 2018) <https://www.theverge.com/2018/4/5/17199210/blockchain-coincenter-

Stan Higgins, "UK Land Registry Plans to Test Blockchain in Digital Push" (2017), <https://www.coindesk.com/uk-land-registry-plans-test-blockchain-digital-push/> accessed 2 April 2019.

Stroz E, 'Psychology Is The Key To Detecting Internal Cyberthreats' (Harvard Business Review, 2016) <https://hbr.org/2016/09/psychology-is-the-key-to-detecting-internal-cyberthreats> accessed 10 June 2019

Vikram Varakantam, '4 Things You Need To Know About SOC 2 Compliance' (Threat Stack, 2018) <https://www.threatstack.com/blog/not-soc-2-compliant-4-reasons-your-customers-wont-work-with-you> accessed 6 August 2019.

Vincent Fauchoux, Bénédicte Chaniot and William Fauchoux, 'How Can Blockchain Revolutionize The Proof Of Existence Of IP Assets Protected By An Unregistered IP Rights Worldwide?' (Blockchainyourip.com, 2018) <https://blockchainyourip.com/wp-content/uploads/2018/12/Blockchain-for-IP-assets-White-Paper.pdf> accessed 21 June 2019

Vindu Goel and Nicole Perlroth, 'Yahoo Says 1 Billion User Accounts Were Hacked' (Nytimes.com, 2016) <https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html> accessed 27 June 2019.