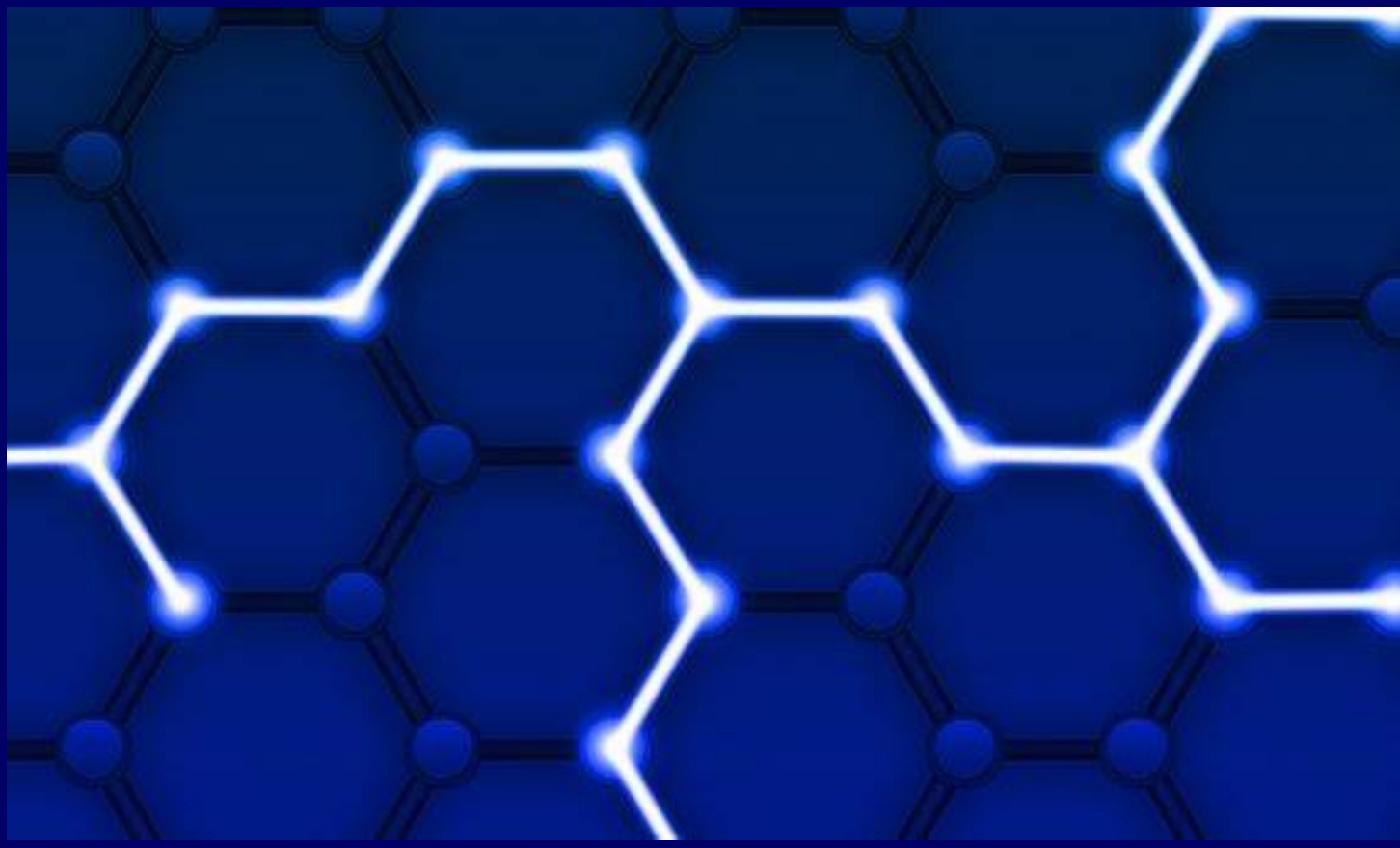
Multidisciplinary Aspects of Blockchain

N H A van Duuren, V A de Pous



Multidisciplinary Aspects of Blockchain

Natascha van Duuren LLM
Victor de Pous LLM (eds.)

ISBN: 978-90-9031867-7
NUR: 820

Index

Foreword

With this special compilation on a fascinating and extremely topical technology, professional association the Royal Dutch Association of Computer and Information Professionals (*Koninklijke Nederlandse Vereniging van Informatieprofessionals*, KNVI) once again gets the ball rolling across several disciplines, as a predecessor, the Dutch Computer Society (*Nederlands Genootschap voor Informatica*, NGI), did earlier in relation to data privacy (in 1982 no less) and to the likewise socially-relevant topic of the vulnerability of the information society in 1987.

Blockchain technology may no longer be a newcomer - the concept stems from 2008 - but that does not mean that we know precisely where and how we should place this technology, while the digital transformation continues at an ever-increasing rate. This prompts all sorts of questions. Blockchain in any event involves information technology that can suffer an outage or be intentionally disrupted through a defect in quality. It is also a system in which participants take part, which means certain agreements are necessary. Generally speaking, as is often the case with new technology and its applications, it is still lacking various frameworks.

Blockchain appeals to the imagination and on these grounds alone is, in KNVI's view, deserving of research. Technologically inclined colleagues look with interest at the enormous computing power required for public blockchain and, for instance, at the mathematical security concept of this distributed and chronological database, whereby changes take place on the basis of consensus. Colleagues who want to see information flowing want to know more about the horizontal and vertical applications of blockchains. Ultimately, it is our digital professionals of all types and disciplines who, based on their up-to-date competencies, are able to use blockchain, in both the public and private sector, and always with a sharp eye for the economic, social and ethical requirements.

There is a crucial role here for the information professional 3.0, therefore. His task is to contribute to socially responsible digitalisation and perform the work ethically, just as a blockchain guarantees the realisation of digital system integrity. That is what KNVI calls *Smart Humanity*. *Human well-being* must also be the priority when using blockchain. Everyone must constantly become acquainted with the ever-evolving information society. At the same time, society must also be able to trust in the information professional.

The KNVI board regards this compilation as an example of the way in which our professional organisation shoulders its social responsibility and tackles complex topics from a multidisciplinary approach; together with both internal experts (from Special Interest Groups and departments) and external experts from various segments of society. Cooperation and knowledge sharing in its purest form.

Wouter Bronsgeest and Paul Baak, Co-Presidents of KNVI Amsterdam, 8 January 2019

Editorial

'First oranges, and now also nutmeg in blockchain', a Dutch newspaper reported recently, referring to a new practical case in the food sector where the digital technology is being used to chart out the cross-border supply chain. The consumer will be able to see, step by step, where the products come from and how they are produced. With transparency on sustainability and quality as the key argument and most likely also in a bid to improve efficiency and control of food security.
Since 20 June 2018, passengers travelling via Amsterdam Airport Schiphol have been able to use a crypto-cash machine to convert their remaining euros into bitcoins or ether; or vice versa. The coins are deposited directly into the traveller's 'wallet'; a maximum of €100 can be converted. This is still a trial for the time being.

After the success of the compilation *Digitaal recht voor IT professionals*[1] [Digital law for IT professionals], the board of the KNVI Special Interest Group IT and Law decided to set their sights on the topical domain of blockchain, where the underlying technology and innovative applications are developing rapidly. The topic is no longer limited to the initial application of cryptocurrencies and a multidisciplinary approach is required in order to identify and evaluate the risks and benefits for businesses and government organisations, for instance. So not only from a legal viewpoint, but in cohesion.

More than any other professional organisation, the Royal Dutch Association of Computer and Information Professionals (KNVI) - particularly after the consolidation with the Ngi-NGN and SOD associations as of 1 January 2017 - unites a broad range of digital professional groups, so that this relatively new and much debated database technology can be approached with joined forces. This is no sinecure, since the subject of study appears abstract, is technically complex and is moreover still fully in development, while the societal, economic and legal consequences are yet to be clearly discerned. Remember that blockchain is still just at the beginning of its life-cycle.

At the moment, this digital technology proves to be a moving target, on which opinions vary. While one category sees blockchain as the most relevant invention since the world wide web of the internet - it's been called the 'ultimate disruptor,' a 'strategic trump card' and a 'game changer' - others view it more as a solution in search of a problem and warn about the hype. In the meantime, there are legion theoretical descriptions as well as different types of blockchain in practice. In our publication, we use blockchain as a collective name for digital databases that are distributed, mathematically secured and chronological in nature, in which registrations take place based on consensus, unless this is deviated from in an individual chapter. As far as the type is concerned, we distinguish roughly between public (open) and private (closed) and between 'permissionless' and 'permissioned' blockchains, although we are aware that different categories could also be used, for example based on other kinds of combinations or more detail.

In addition to horizontal and sectoral applications, such as identity or healthcare, respectively, attention is devoted to societal, technical and legal aspects of blockchain.
It goes without saying that we are grateful to all the authors who together made this compilation possible. The individual contributions were written in a personal capacity and were deliberately kept

[1] V.A. de Pous (ed.), *Digitaal recht voor IT professionals*, Amsterdam, 2016.

concise in nature. (In the event of multiple authors, the authors are listed alphabetically.) They contain valuable analyses and suggestions, but no advice for concrete cases. Above all, the texts unlock the insights and knowledge of today. Given the speed at which blockchain, its applications and aspects are developing, adaptation and expansion will most likely be unavoidable sooner rather than later. We are happy to take on this task as well.

For now, our SIG assumes that the compilation contributes to the multidisciplinary knowledge sharing on this topic. It can benefit people already involved in blockchain or considering using the technology for their organisation. The work also provides background and reference points for politicians, who are being confronted with policy questions in this area.

Natascha van Duuren and Victor de Pous Amsterdam, January 8, 2019

1 Societal and economic perspective

Victor de Pous

Anyone looking back on recent history can see that the expectations for ICT have invariably been high. The expectations for data-processing models, such as mainframe, client/server, cloud and edge computing, and for the countless technologies and applications. Today, the Internet-of-Things, big data, artificial intelligence and robotisation are making headlines as part of a unique transformation: the change taking place as digital technology is applied in all aspects of our society. Blockchain has joined these. Blockchain is the collective name for digital databases that are distributed, mathematically secured and chronological in nature. In theory, the technology has the capacity to resolve a widespread problem: *the lack of trust in digital systems*. At the same time, blockchains - either incidentally or, increasingly, with premeditation - can initiate new business and process models because they unlock a *different way of organising*, thanks to the unalterable registration of traceable data without a *trusted third party*.

Napster

Back in time. Peer-to-peer systems - distributed software systems that consist of nodes and which make their sources, such as computing power or storage, directly and autonomously available to each other - existed both in theory and practice years before Napster made it possible to share MP3 music files via the Internet in June 1999. With all the ensuing consequences. The large-scale use of this open P2P network without administrative authorities and restrictions disrupted the record industry. The US company grew exponentially, from 0 to 80 million registered users, but had to shut up shop in July 2001 on grounds of copyright infringement.

What we call blockchain pertains to peer-to-peer systems. It is a new decentralised, secure and chronological database technology to synchronise stored data on the basis of consensus. This kind of system was first described as an application for electronic coins in 2008, by Satoshi Nakamoto; a pseudonym.[2] A year later the first bitcoin was 'mined', by a person or persons whose identity is still not known. In January 2018 there were approximately 1,300 different cryptocurrencies, according to De Nederlandsche Bank. Six months later that number had grown to more than 1,600.[3]

High expectations

It is not only the usual suspects - predictors of the future and innovative entrepreneurs - who are enthusiastic. Dutch Minister Sigrid Kaag (Foreign Trade and Development Cooperation) also had no doubt about the importance of the technology on 21 April 2018. So-called 'transformative technologies' can make the difference for international development and financial inclusion. '*Blockchain is such a new technology and it offers tremendous opportunities. For business, for the public sector, and for development cooperation*'.[4] Enormous opportunities, and for everyone. Colleague Wopke Hoekstra (Finance) took a

[2] https://bitcoin.org/bitcoin.pdf

[3] https://en.wikipedia.org/wiki/List_of_cryptocurrencies

[4] https://www.rijksoverheid.nl/documenten/toespraken/2018/04/21/toespraak-minister-kaag-bij-voorjaarsvergadering-imf-en-wereldbank

more cautious approach. He wants to *retain the technology's potential* when bringing cryptocurrencies into an 'appropriate' (international) regulatory framework (and in doing so prevent improper use), according to his letter to the Lower House of Parliament dated 8 March 2018.[5]

One month later, state secretary Mona Keijzer (Economic Affairs and Climate) said that much of the potential of blockchain still needs to be achieved, but that '*blockchain is a good example of a potentially disruptive innovation, it could be a game-changer*.'[6] De Nederlandsche Bank: this regulator believes that the technology behind bitcoin and others of its ilk is 'interesting and possibly very promising' (and for the time being does *not* classify cryptocurrencies as money, with reasons).[7] What does this opportunity or (disruptive) promise look like and on what are these viewpoints based?

Trust through technical integrity

Blockchain has a number of features, at least two of which are very striking. The *recording and validation* of data (mainly on ownership) which are *unalterable* and *traceable* is key. The technology is principally intended to 'achieve and maintain integrity in distributed systems.'[8] It is generally asserted that parties that do not know each other can, without the intervention of a third party (the traditional 'trusted third party' - TTP - such as a bank, civil-law notary or government organisation, such as the Land Registry or RDW (National Vehicle and Driving Licence Registration Authority)), enter into a reliably executed transaction via a blockchain.

The new data-processing method could be applied in many areas, such as financial matters (payments, loans), the issuing of official documents (passport, ID card, driving licence, educational certificate, patent granting, registrations in the Land Registry, Chamber of Commerce registrations), the origin of products (for each step in the supply chain), verifying digital identities, and, for instance, the automated and guaranteed performance of a contract (smart contracts). More generally, blockchain will prove useful if the (legal) *irrefutability and traceability* of the data registration is a societal or economic basic condition.

Caution is nonetheless advised, warns the authoritative US National Institute of Standards and Technology: '*There is hype around the use of blockchain technology, yet the technology is not well understood. It is not magical; it will not solve all problems. As with all new technology, there is a tendency to want to apply it to every sector in every way imaginable.*'[9]

Organising differently without an intermediary

Another striking particularity is the capacity to organise a business, process or part thereof differently. That is not unique to blockchain, incidentally. ICT has long been unlocking new organisational models, thanks in part to telecommunications, computer networks and mobile connectivity. Take, for example, what operating independent of place and time ('virtually') has achieved, such as new ways of working.[10] The oft-cited aspect of *disintermediation*[11] also cannot be called unique. Online flight ticket sales by

[5] https://www.rijksoverheid.nl/documenten/kamerstukken/2018/03/08/antwoorden-kamervragen-over-%E2%80%98franse-regering-wil-strengere-regels-voor-bitcoin%E2%80%999

[6] https://www.rijksoverheid.nl/documenten/toespraken/2018/04/09/toespraak-van-staatssecretaris-keijzer-economische-zaken-en-klimaat-tijdens-digital-day-in-brussel

[7] https://www.dnb.nl/binaries/Position%20Paper%20DNB%20Cryptocurrencies_tcm46-371493.pdf

[8] Daniel Drescher, *Blockchain basics, A non-technical introduction in 25 steps*, New York, 2017.

[9] https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf

[10] On the history and legal aspects of the new way of working, see V.A. de Pous, *Digitaal werken [Working digitally]*, in V.A. de Pous (ed.), *Digitaal recht voor IT professionals*, Amsterdam, 2016.

[11] https://en.wikipedia.org/wiki/Disintermediation. Removing the intermediary in the supply chain and in transactions.

airlines have largely forced the travel agent as intermediary to disappear. In fact, virtually everyone who offers a product or service via the internet these days bypasses the wholesaler, distributor and shop, as they see fit.

With blockchain, the intermediary that has been programmed away or who perhaps never existed is of a particular type, however: a *central authority* (TTP).

Payoffs

As a result of the *digital system integrity*, blockchain is, on the one hand, a trust-creating technology (due to the unalterability and traceability of the data processed) and on the other potentially 'disruptive' in nature for the economy and/or sectors, because established 'institutions' can become superfluous. This dual perception prevails by and large. For instance, state secretary Keizer bases the alleged game-changing capacity of blockchain on three grounds: the technology 'gives people a sense of autonomy in the sometimes chaotic online world', it 'reduces the administrative rigmarole' and it 'creates trust between parties'.

Or take Air France-KLM. The airline wants to use blockchain technology to 'revolutionise' the contacts with the travel sector for customers, businesses and start-ups so that the relationship becomes more personal and the customer experience is improved. But this step will also achieve savings on costs.[12] Yet another application. Regulator DNB sees potential opportunities for a blockchain which records each step in the food chain for a particular food. Incidentally, that is already taking place for oranges, nutmeg and chocolate.[13] If one zooms out a bit here, we see that the technology can significantly improve transparency, safety, efficiency and quality in supply chains.

Conditional suitability

With the umpteenth hyped digital invention, the question traditionally arises of whether a 'technology push' or 'market pull' is involved. Based on the pioneering work of the mysterious Satoshi Nakamoto, we can conclude that as far as we can tell, the technology was suddenly there, without market research, which argues for the idea that it is a push (a technology looking for a problem), while given the many initiatives and projects worldwide and in all sorts of sectors, it can probably be just as easily assumed that the market demand (for digital trust and/or another way of organising) evidently existed; albeit latently. 'You will only see it once you understand', said Johan Cruijff.

Perhaps the answer also depends on the sector. By its own admission, DNB has built four prototypes of a cryptocurrency based on blockchain in order to better understand the technology. Experimentally, therefore. According to the regulator, the outcomes confirm 'that the technology is not yet mature enough to play a role in our payments traffic (too slow, too few transactions per second, not sustainable), but is indeed interesting and could perhaps in time offer possibilities for transactions in the financial world and beyond.'[14] Some in the Netherlands are already talking about a 'fundamental' technology.[15]

This brings us to generic, sector or application-independent criteria for a blockchain application in practice. *When or for what is blockchain actually suitable?* SURF, the ICT cooperative organisation of education and research in the Netherlands, pointed to the following criteria in a technology survey from November 2017.[16] Summarised here: (i) the parties must distrust each other in terms of the integrity of

[12] http://finteknews.com/air-france-klm-turning-to-blockchain-to-cut-costs/

[13] Not every experiment succeeds. https://www.coffeepro.nl/nl/nieuws/tony-chocolony-stopt-blockchain-experiment

[14] T.a.p. note 5.

[15] Like the Smart Contract Working Group of the Dutch Blockchain Coalition.

[16] https://www.surf.nl/kennisbank/2017/technologieverkenning-blockchain-voor-surfnet-en-haar-achterban.html

the (administrative) data processing, (ii) the current TTP is not satisfactory (too expensive, too slow, unreliable), (iii) transparency is a condition or may not pose any (legal) impediment, (iv) multiple independent parties must create blocks (because otherwise the blockchain has no added value above a TTP), and (v) a sound business model is required (because otherwise participants will stay away on account of high investments and operational costs in order to get adequate computing power).

At this time, we propose that the evaluation process should in any event start with the question of whether parties actually *want* to cooperate, particularly for supply chain blockchains. This sounds like a no-brainer but should not be taken for granted. A survey among 1,500 European companies shows that 83% expect a great deal from blockchain applications, but that just 2% are willing to work with others on this. The rest apparently do not want to share knowledge.[17]

Conclusions

'Money matters without the bank' is how School-TV described blockchain.[18] It is difficult to state more concisely what a practical application of a blockchain would in theory encompass. Proponents always point to the creation of trust and reduction in bureaucracy. Pragmatics, who are not diametrically opposite this position, but rather diagonally, are moderately positive about blockchain and in principle are keeping an open mind, partly because this - composite and complex - information technology is not yet adequately clear, technically or otherwise.

Actual opponents seem to be few, but might be found among the existing trusted third parties, such as central authorities. The negative environmental effects of the public and permissionless blockchain model are frequently pointed out, however, because 'mining' tokens requires an extraordinary amount of computing power and therefore energy. Other objections, or perhaps more accurately, functional limitations and design requirements, are based on the existing legal frameworks. To name two legal clusters: regulations for the processing of personal data and regulations relating to agreements: the law of contracts. But the law is much broader, of course.

Analyses

- We would expect that politicians, just given the many divergent and parallel changes in our society brought about by digitalisation[19], would be reticent about economic or sectoral disruption because stability is so important. Dutch government members are embracing 'transformative technologies' but there has been little talk of conditions or preconditions, perhaps with the exception of the general desire that there be adequate 'cybersecurity'.

- Lawfulness is a *conditio sine qua non* for every blockchain application. From the development phase (usually open source software) through to the production environment (also cross-border). Everything must be in accordance with the legislation governing privacy, contracts, security, finance, tax, identity, and, for instance, evidence.

- Furthermore, economic disruption must also take place lawfully, i.e. blockchain may not disrupt any 'level playing field' or, as the case may be, may not be in contravention of economic law or competition law. Napster's innovative P2P application for sharing music files online was in any

[17] https://www.techzine.be/nieuws/19945/europese-bedrijven-willen-niet-samenwerken-rond-blockchain.html and https://www.cognizant.com/whitepapers/blockchain-in-europe-closing-the-strategy-gap-codex3320.pdf

[18] https://schooltv.nl/video/wat-is-blockchain-geldzaken-zonder-bank/

[19] Adjacent to this: there is growing criticism of the digitalising government from the National Ombudsman, Consumentenbond (Consumers' Association) and the Council of State.

event unlawful under US copyright law, which was confirmed at a later point in time by the highest court of the United States.[20]

- Blockchain applications are only operational when the network is available. Telecommunications disruptions in the European Union are primarily (62%) caused by (i) software errors and (ii) defective hardware, according to an analysis by ENISA, the European agency for network and information security.[21] Digital attacks accounted for just 2.5% of incidents in 2017. The figures point to a general sore spot of the information society: *inadequate digital quality*. If this technology aims to create trust through intrinsic system integrity, it may not be lacking in quality.

[20] In MGV v. Grokster (545 U.S. 913 (2005)) the Supreme Court decided that the developers of peer-to-peer networks could be held liable if this software was offered as a means for infringing copyrights.

[21] https://www.enisa.europa.eu/news/enisa-news/169-telecom-incidents-reported-extreme-weather-major-factor

2 The first scope of application: cryptocurrencies

Laurens Thissen

There is no denying that blockchain is a new IT hype. Some even seem to assign intrinsic value to blockchain. Just as others assigned such value to 'the Cloud' during the last decade and to the internet at the end of the 1990s. But, as always, time will show that it is not the technology itself which has (intrinsic) value, but that the value lies in applying the technology. Blockchain technology promises to have a number of valuable, even disruptive possible applications. The most sweeping promise is that blockchain will make our trusted third parties, such as banks, civil-law notaries, certification authorities and certain government authorities, etc., superfluous. In many, if not all, areas, this technology first has to prove itself, however. But virtual currencies are already well on their way.

What are virtual currencies?

Virtual currencies – also referred to as cryptocurrencies or 'cryptos'[22] - is a collective term for blockchain applications in which the crypto, whose units are referred to as 'coins', serves as a means of payment.[23] Well-known examples include Bitcoin, Litecoin, Ether and Ripple. Cryptos are issued in an 'initial coin offering' (ICO). The crypto-issuer tries to attract investors, who receive cryptos in exchange for their investment. The issuer usually publishes a white paper explaining why the investment is an attractive one.

The informal character of the ICO is typical. This is in stark contrast to the initial public offering (IPO) of shares on a market. After all, strict legislation and regulation applies to the IPO process and the process is subject to supervision by regulators, in order to determine, among other things, how many shares are offered for sale and at what price, for instance. To that extent, an ICO still most resembles a form of crowdfunding. But certainly a successful one. On the reference date of 17 October 2018, the counter for 2018 was already at 894 ICOs, whereby a total of USD 21,356,115,254[24] had been raised.

A cryptocurrency is not money

People should realise that cryptocurrency is not 'money' in the sense of legal tender. According to the European Central Bank, it does not have the characteristics of money: it is not issued by a (recognised) central authority, for instance, and is not a generally accepted means of payment. The Dutch government, central bank and financial markets regulator (AFM) agree with this position.

The traditional financial sector is highly regulated. The issuing of official means of payment is reserved for the state - as it should be; banks are bound by a materially demanding licensing requirement, financial products are subject to all sorts of restrictions, particularly also laws and regulations to protect consumers, and De Nederlandsche Bank and the AFM supervise this branch of industry closely. A consequence of not recognising cryptos as legal tender is that the aforementioned

[22] Strictly speaking, virtual currency is the collective term for money that only exists virtually or digitally, and also includes 'cryptographic currency'. 'Cryptographic currency' is money based on blockchain and cryptography and is referred to in this article as 'crypto'.

[23] Blockchain technology can assign more than just monetary value to cryptos. In addition to coins, there are 'tokens', which can have (infinitely many) other functions than just the exchange of monetary value. For instance, tokens can encompass rights, certificates, titles, smart contracts, etc. Cryptos as discussed in this article can be interpreted as 'coins' or 'payment tokens'. Other tokens, which can be categorised as utility tokens or asset tokens, fall outside the scope of this article.

[24] Source: www.coinschedule.com/stats

legislation and the current tax/civil law does not apply to cryptocurrencies, or at least not automatically. Bitcoin has, incidentally, been recognised in the case law of (lower) Dutch courts as a 'means of exchange'.

Valuation

Money in its oldest forms never left any doubts about its value. After all, the Roman soldier of yore could easily estimate the value of his monthly wage, paid out at the time in scarce salt (in Latin: *salis*, which later evolved into 'salary'). As could people later on in history, whose claim on a share in gold holdings was evidenced by a note, and by people now who have a (virtual) claim on the bank.

The value of a cryptocurrency is harder to determine. Unlike the value of a share, the value of a crypto does not correlate (measurably) to the value of a business. The value of the crypto is based virtually entirely on the confidence that exists in the (organisation and business case behind the) crypto and the (adoption of the) possibilities for application it presents. Because blockchain and therefore cryptocurrencies as well seem to have unlimited application possibilities, there are different business cases behind the different cryptocurrencies and investing can be attractive for various reasons. This applies all the more if the issuer of the cryptocurrency is backed by an organisation (or consortium of organisations) that enjoys a measure of trust in its respective industry. The common denominator of all cryptocurrencies is that after the ICO, the issue of new cryptos is impossible or limited, after which the crypto can be traded. The value of the crypto is subsequently determined based on good old demand and supply.

Role in economic transactions

Unlike in certain developing countries where Bitcoin is more trusted and is therefore preferred above the local currency as a means of payment, there has not yet been wide adoption of cryptocurrencies on the Dutch market. The legitimate transactions that are settled in the Netherlands using these means are perhaps still negligible compared to euro transactions. But the point is that *there are indeed transactions being settled in cryptos*, and the transactions are growing in both number and value. As the technology develops and improves, acceptance and adoption will grow. And as adoption grows, cryptos will assume an increasingly important role in (international) payments. Cryptos are here to stay; this is a factor which must undeniably be taken into account socio-economically and legally.

Regulation?

As stated, the regulation for the traditional financial sector does not apply to cryptocurrency. Regulations are conspicuous by their absence when it comes to cryptos, therefore. Anyone who considers themselves capable (rightly or otherwise) can therefore issue a crypto. And in the absence of any intrinsic value of the crypto, the value is determined by the confidence that the market has (however well-founded or misplaced) in the particular coin (i.e. in the business case or organisation behind it). Or simply by whatever some loon will pay for it. That could be a great deal, as is presently the case for Bitcoin, or (virtually) nothing, as is the case for many other cryptos.

It is precisely because of the legal limbo surrounding cryptocurrencies, in combination with their growing importance and the potentially disruptive applications, that regulation will be needed in the long term. International, European and Dutch financial regulators still have a sceptical, wait-and-see attitude when it comes to cryptos. The initial trivialising of cryptos by the regulators, because they are reportedly used by just a small group, has since made way for repeated warnings about the risks. It therefore seems that the regulators have also gradually come to the realisation that the regulation of cryptos as a financial asset is both desirable and necessary. Political calls for regulation are also being heard.

Laws and regulation

Legislative initiatives in the Netherlands and in the European Union are still in the exploratory phase. The European Securities and Markets Authority takes the view, for instance, that ICOs fall under the European directives already in force.[25] The practicality of this seems limited in the Netherlands, however, since the AFM has hinted that ICOs can be set up so that they fall outside the formal and material scope of application of the Financial Supervision Act, which is based on the aforementioned directives. In order to legally interpret an ICO and cryptocurrency, therefore, case law must be relied on, mainly from lower courts, which, on the one hand, is extremely casuistic in nature and, on the other, produces different outcomes in different jurisdictions. This latter effect is due in part to the fact that some states, including certain EU member states, have indeed regulated cryptocurrency to a greater or lesser extent, though not in the same manner. To mention two extremes: some countries have already introduced their own 'state crypto' with related regulatory legislation, while other countries have a total ban on trading in cryptos.

There are also no concrete initiatives at the global level. Even though regulation at the global level, via bilateral or multilateral treaties or otherwise, is in fact desirable. After all, payments travel across borders. Legal certainty is essential for international commerce. And international differences in legislation are not conducive for legal certainty, to put it mildly. It would even be disastrous for legal certainty if payments in cryptocurrencies were to have different (legal) effects from country to country or were not regarded as payment in discharge of an obligation in certain countries. This therefore requires not only regulation of cryptos as part of the financial market, but also regulation (or better: recognition) of cryptos in private law.

Adoption of the technology dictates the standards

The fact that firm regulatory initiatives have not yet emerged is not surprising in and of itself. The technology is relatively young and still evolving. Different blockchain programmers still use different definitions of blockchain, for instance, and certain blockchain practical cases sometimes do not even satisfy the definition of blockchain used by the particular blockchain programmer himself. In the absence of consensus in the crypto community and given the evolution that cryptos will undoubtedly still undergo, it cannot presently be determined which crypto technology, or variant thereof, or application thereof, will be adopted by the market, and therefore what degree of regulation and what regulatory regime will be desirable. Such consensus and the ensuing widespread support from the crypto community itself, the business sector and later politics will still have to precede any concrete international regulation.

Insights

- Cryptocurrencies are globally the most widely adopted practical case of blockchain technology and seem to have secured a permanent place in socio-economic commerce.

- Because of the - growing - importance of virtual currency in commerce and the potentially disruptive uses of the technology, regulation seems necessary.

- The legal certainty that is essential for international commerce necessitates regulation at the international level, both in relation to virtual currency as part of the financial markets and in private law.

[25] Directive 2003/71 (Prospectus Directive), Directive 2014/65 (Markets in Financial Instruments Directive), Directive 2011/61 (Alternative Investment Fund Managers Directive) and Directive 2015/849 (Fourth Anti-Money Laundering Directive).

- Depending on how crypto technology and its applications evolve, crystallise out and are adopted by the market, the need for regulation can be materially assessed.

3 Digital competences for blockchain

Liesbeth Ruoff–van Welzen

Like many other technical innovations, there are still very few accepted descriptions of the skills, competences and knowledge required to use blockchain. This decentralised database technology is often discussed in master classes, short-term training courses and seminars, where early adopters, developers and users share their experiences and findings while discussing use cases in practice. In this article, we describe the results of a search for the skills and competences of mostly Dutch early users in terms of their digital skill profiles, and the lessons we can learn from them. We start by providing relevant background information in the context of the discussions about digital skills in the European Union.

The context

A new digital technology such as blockchain generally requires a long lead time, partly because of its immature character. Important features during the maturing process of an innovation include acceptance and trust by its users by demonstrating its effective use. How is trust achieved in these digitised processes? One thing is certain: it is not enough just to test the technology. Added to that, the talents and educational background of the people involved in building and using the technology also play an important role.

It was Paul Strassmann who drew our attention to the importance of *human capital* in his book *Information Productivity; Assessing the Information Management Costs of U.S. Industrial Corporations.*[26] He came to the conclusion that an organisation's investments in employees with suitable skills were higher than those in hardware and software. On the other hand, he also concluded that these investments in human capital were much more profitable, i.e. the returns were higher[27].

There is a growing focus on digital skills in Europe. For the first time the *ICT Rolling Plan for ICT Standardisation*[28] includes e-skills and e-learning as subjects. Based on this plan in Europe, a budget can be allocated in the multiannual plan[29]. The e-Competence Framework or e-CF[30] constitutes the basis for the standardisation of e-skills and e-learning in the European Union. This framework has a long history. In 2002, the first steps were taken to investigate and discuss the growing gap between supply and demand for digital skills in the European market. It appeared necessary to develop a single common definition framework for referring to digital skills in the European countries and to resolve any discrepancies.

In 2016, e-CF was established as a standard. In that framework (version 3.0), 40 generic competencies were defined in five competence areas, i.e. (i) plan, (ii) build, (iii) run, (iv) enable and (v) manage. In the definition of the competences, links can be made to Components of knowledge and

[26] http://www.infoeconomics.com/info-productivity.php

[27] http://www.strassmann.com/pubs/computerworld/rankings/ip_rankings_v3.pdf

[28] https://ec.europa.eu/growth/content/2018-rolling-plan-ict-standardisation-released_en

[29] https://ec.europa.eu/digital-single-market/en/news/digital-single-market-mid-term-review

[30] http://www.ecompetences.eu/

skills and to Role profiles[31]. The European Commission formulated 30 of these links. Tools were developed to deal with the following links from e-CF:

- a switch from the profiles to job descriptions in ESCO, the language used by all European countries to communicate about the labour market;
- a mapping to the learning levels of the European Qualifications Framework;
- a list of results of a project or activity, which makes it possible to switch to competences;
- links were made to SFIA[32] and the RACI[33] model.

Worldwide, the independent and non-commercial development of ideas related to digital skills has its place in IP3[34] as part of IFIP[35]. IFIP is the Worldwide Federation of national IT professional organisations, similar KNVI in the Netherlands. The cooperation of IP3 engenders trust in the accreditation and certification process. From the start, SFIA was used as a basis for the descriptions of digital skills, but IP3 also established[36] the e-CF framework, as appeared at WCC 2018 in Poznan[37].

In the Netherlands we have the public-private Dutch Blockchain Coalition, which focuses on reliable and socially accepted blockchain applications.[38] A human capital agenda is now available that specifies which knowledge, skills and behavioural competences can be requested in the various domains relevant to blockchain. Many different suppliers and customers are involved in blockchain.

One particular blockchain ecosystem description in the Netherlands distinguished seven different segments among the customers and nine among the suppliers[39]. The spectrum ranges from providers of cryptocurrencies to financing, with, among others, the technical developers in between. Trust cannot exist without mutual understanding. All players on both the supplier and customer sides will require digital skills to understand each other and use this new solution together.

Blockchain digital skills

For our search, we looked at the digital skills, competences and other skills of Dutch early users, all of whom are affiliated to the Dutch Blockchain Coalition. We used the e-CF framework and the e-CF® NEXT developed by EXIN[40]. The first striking findings can be described as follows:

1. All profiles have four e-CF competences in common: (i) Technology Trend Monitoring, (ii) Information and Knowledge Management, (iii) Relationship Management and (iv) Business Change Management at the highest levels[41].
    a. Among these competences, the following skills play a role:
        i. identifying commercial benefits and improvements using new applications
        ii. collecting internal and external knowledge and information needs
        iii. creating realistic expectations to support the development of mutual trust

[31] –Part 2: User Guide: http://www.ecompetences.eu/ict-professional-profiles/

[32] www.sfia-online.org

[33] . http://www.valuebasedmanagement.net/methods_raci.html

[34] https://www.ipthree.org/ IP3, the 'International Professional Practice Partnership' is leading the development of the ICT professions group worldwide.

[35] International Federation for Information Processing (IFIP). http://www.ifip.org/

[36] https://www.ipthree.org/knowledge-portal/

[37] https://www.ipthree.org/knowledge-portal/wcc2018-frameworks/

[38]https://www.cencenelec.eu/News/Brief_News/Pages/NEWS-2016-023.aspx

[39] Blockchain ecosystem, version 0.7, June 2018, Economic Board Utrecht

[40] https://www.exin.com/e-cfr-next?language_content_entity=nl

[41] http://www.ecompetences.eu/wp-content/uploads/2014/02/European-e-Competence-Framework-3.0_CEN_CWA_16234-1_2014.pdf

iv. analysing the costs and benefits of the implementation of new ICT solutions.

b. The knowledge component in these competences includes:
   i. knowledge of organisational processes – both internal processes and the processes of customers – including decision-making, budgeting and management structure
   ii. understanding the impact of new ICT solutions on business processes
   iii. understanding the impact of new ICT solutions on the organisation and employees
   iv. understanding the legal implications of new ICT solutions.

2. At least two approaches are possible: skills and knowledge exist either from the perspective of electronic engineering / networks or from documents / information processing.
3. The role in the organisation is important in determining the necessary digital skills. For example, is it the role of the blockchain application builder or introducing / supporting its implementation – that is, when using or managing blockchain in an organisation?
4. A thorough knowledge of an industry or professional group is also necessary to ensure success.
5. An understanding of network and information security in general and cryptography in particular is also necessary.

In general, it can be said that at senior level the first users and developers of blockchain applications in the Netherlands are characterised by a wide range of competences. A translation of these findings into currently available talent should not be a problem.

Ambition but no policy

The abundance of existing and impending digital laws and regulations and digital policy notes by the new government is testimony to its ambition. After the *National Cyber Security Agenda* of 21 April 2018, which included seven 'solid' ambitions, and the *Dutch Digitisation Strategy* of 3 June 2018, the strategy of '*The Netherlands Digital*' is now in place. This strategy was made public on 16 June 2018 by State Secretary Keijzer (Economic Affairs and Climate), Minister Grapperhaus (Justice and Security) and State Secretary Knops (Home Affairs and Kingdom Affairs). The main focus was on the following three ambitions:

- leading the way and taking advantage of opportunities;
- getting everyone to join in and cooperate;
- building trust in the digital future.

The situation on the ground is very different. The task of maintaining digital skills is left entirely to employers and employees[42]. The memorandum recognises, for example, that small and medium-sized businesses are traditionally the job engine of the Dutch economy and at the same time notes that the possibilities of digitisation are not sufficiently used[43]. It is argued that 'Entrepreneurs, amongst others, say that they don't know which digital innovations give them the best return and how to implement them.' Paul Strassmann's research[44] showed a long time ago that investing in *human capital* yields the highest return.

[42] P. 31 in 'Nederland digitaal' [The Netherlands Digital']
https://www.rijksoverheid.nl/documenten/rapporten/2018/06/01/nederlandse-digitaliseringsstrategie

[43] P. 17 in 'Nederland digitaal' [The Netherlands Digital'].

[44] Ref. to notes 1, 2.

Government policy to fill this gap has *not* been formulated in the Dutch Digitisation strategy. For example, the ambition 'Trust in the digital future' has not been translated into a structural policy to continuously maintain digital skills across the full scope of Dutch society and increase them, where necessary. Without sufficient knowledge, trust will not be easy to develop.

The European Union

In Europe, initiatives are being taken in the field of digital skills. In addition to competences, the European standards committee CEN / TC 428[45], *ICT Professionalism and Digital competences* (formerly the E-competences standards committee), now also deals with ethical standards, ICT knowledge, training curricula and certification. CEN / TC 428 shows that the maturing of the ICT profession is supported in all sectors, both public and private. Standards contribute to this and serve as a basis for taking national and international action.

Conclusion

The findings and description of the Dutch situation are the first step towards achieving the necessary digital skill sets in the blockchain domain[46]. It is not merely new skills that are needed; seniority and experience with various blockchain components are also required so that the possibilities of this technology are embedded in order to successfully transform business processes.

In addition, Dutch government policy will soon have to recognise the importance of digital skills for both customers and blockchain application providers. The competitive position of the Netherlands, especially in the blockchain area, depends on the digital skills of the builders, implementers and inventors of blockchain applications. It is still too early to talk about objectively testing and assessing these digital skills.

Points of focus

- The parties concerned must realise that blockchain digital skills currently consist of a combination of previously acquired competences, with newly acquired experience and knowledge.

- The importance of digital skills to enable IT professionals to stand out in the international market must be acknowledged.

- Do not focus purely on digital skills, but take a broader perspective as a starting point. This applies to both the providers and the customers of blockchain applications.

- Internationally trusted and acknowledged frameworks for digital skills offer a good handle for gaining the right skills and thereby creating trust in organisations and externally in society. Objectively testing and assessing these skills is a necessary next step. Unfortunately, we are not yet that far, certainly not in the Netherlands.

[45] https://www.cencenelec.eu/News/Brief_News/Pages/NEWS-2016-023.aspx

[46] A summary of all currently specified skills in the blockchain domain: https://patrickmn.com/security/why-blockchain-is-so-hard-to-understand/.

4 Blockchain from a cybersecurity perspective

Jan Nienhuis

Blockchain technology is capable of changing the world and has apparently already started to do so. At the same time, digital threats such as digital burglaries, data leaks and theft are increasing. Privacy and information security are therefore important issues in our society. The protection of electronic data – cybersecurity – traditionally starts with risk awareness. A single protection measure in itself is insufficient to cover any risk. These principles also apply to blockchain applications, as the cryptography at its base is constantly evolving. A system considered safe now may be deciphered within minutes in a few years' time. The challenge is to keep up with developments. The biggest security risk for a blockchain is private key management.

Basics

In the field of information security, cybersecurity involves the protection of electronic data. Cybersecurity starts with risk awareness. Which data cannot be missed, made public or accidentally changed? What are the consequences? What is the probability of an incident? A risk profile is used to create a data classification. This analysis produces guidelines for proportional measures. Then technical solutions are usually purchased and implemented.

One possible measure is the use of a blockchain. However, it is considered unwise to depend on a single security measure. A package of measures and techniques is usually applied according to the principle of *defence-in-depth*.[47]

In this article, we work on the basis of the "*CIA triad*". CIA in this context stands for Confidentiality, Integrity and Availability. These are the core concepts of information security. The balance of these three aspects defines the nature and scaling of security measures for a given data set, classification or process. Later in this chapter, cybersecurity by and for blockchains will be reviewed from these three perspectives.

For a proper analysis of the security properties of blockchain technology, it is important to focus on the objective of the design: a decentralised, public ledger (*distributed ledger*) whose purpose is to validate and record transactions. Three conditions must be met: transactions must be verifiably unique, the unique transactions must be certified and the transactions must be distributed to the participants. All three are accomplished using cryptography, which is the basis of any blockchain.

[47] (ISC)2. (2015). *Official (ISC)2 Guide to the CISSP CBK (fourth edition).* Boca, Raton, London, New York: CRC Press

Asymmetric cryptography

Unicity in blockchains is achieved through asymmetric cryptography, which is a proven technology. Every participant in the blockchain owns a key pair: two cryptographic keys, consisting of very large figures with a specific mathematical relation based on, for example, discrete logarithms or elliptic curve equations.[48] The *private key* is kept secret by the owner; the other key may be shared (*public key*).

The data encrypted with the public key can only be decrypted by using the private key. The public key could be regarded as an electronic padlock, and the private key could be regarded as its key. In Figure 1[49], Alice sends Bob her public key (as an 'open padlock'), Bob uses it to encrypt the message, then sends it to Alice. Alice then uses her private key to decrypt the message.

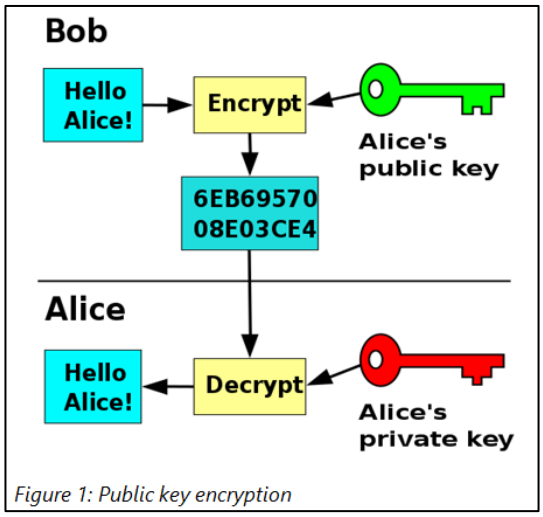


Figure 1: Public key encryption

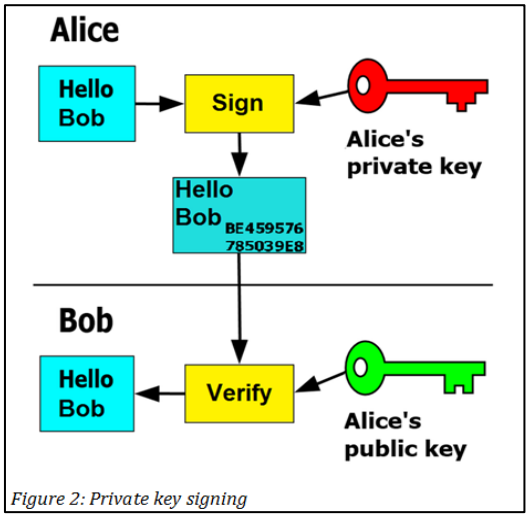


Figure 2: Private key signing

Asymmetric cryptography involves complex mathematics. This would slow down data processing, making it suitable for small amounts of data only. Asymmetric cryptography is therefore often used to generate or exchange symmetric encryption keys[50] (such as the Diffie-Hellman or RSA algorithms).

Blockchains also rely on a system of digital signatures. Alice may generate a signature by performing a calculation on the message and her private key. The result is attached to the message to Bob. Bob uses the corresponding verification algorithm to check Alice's signature. If Bob's calculation produces Alice's public key, he has mathematical proof that the signature was generated using Alice's private key (figure 2[51]). In this way, Alice uses her private key to state her identity, without revealing the key. *'This is an essential part of what makes [blockchain] unhackable. There are no passwords or private keys stored on [blockchain] itself for an attacker to compromise, and yet users can still authenticate transactions.*[52] In a blockchain, every transaction is generated using the recipient's public key and signed using the sender's private key. By adding a timestamp, the transaction becomes unique.[53].

It is vitally important to protect the private key. The loss of this key means the loss of any and all transactions signed with it. When stolen, the transactions in which the key was used are at the thief's

[48] https://resources.infosecinstitute.com/mathematical-algorithms-asymmetric-cryptography-introduction-public-key-infrastructure/

[49] https://en.wikipedia.org/wiki/File:Public_key_encryption.svg#filelinks

[50] Symmetric cryptography uses one key to encrypt and decrypt a message.

[51] https://en.wikipedia.org/wiki/Public-key_cryptography#/media/File:Private_key_signing.png

[52] https://www.investinblockchain.com/how-does-cryptography-protect-blockchain/

[53] https://www.quora.com/How-cryptography-is-used-in-blockchain

disposal.[54] Large amounts of money may be lost in such a situation, as illustrated by the recent death of Quadriga's owner[55].

Chain of hashes

A cryptographic hash function is an algorithm that produces a binary fixed-length string from variable input. In addition:

- the same input will always produce the same hash;
- a hash can be quickly calculated;
- the input can only be recovered by trying out all the possibilities (one-way function);
- a minor change in the input results in a completely different hash;
- different input resulting in the same hash is a rarity.[56]

Hash functions are used to anchor transactions to the ledger. Several transactions are combined in a *block*. A hash is generated for every transaction.[57] A verification hierarchy of hashes-from-hashes is used, known as the Merkle Tree[58]. Thus, any transaction in the blockchain can be verified by following the path down the Merkle Tree. The last resulting hash of the tree (*Merkle Root*) is added to the block header, which contains meta information about the block such as:

- the block version number;
- the timestamp;
- the hash of the previous block;
- the nonce (see below);
- the Merkle Root.

Referring to the previous block forges the chain that effectively gave blockchain technology its name. To prevent the creation of multiple versions of the blockchain in the distributed environment, a *consensus algorithm* is required. The most commonly used consensus algorithm is the Proof-of-Work algorithm (used by Bitcoin, Ethereum and Dash). The nodes in the blockchain verify transactions and solve puzzles[59]. The solution of the puzzle is the *nonce*. Once the hash (Merkle Root + nonce) satisfies the consensus algorithm criteria, the new block is added to the chain.

Blockchains are designed to be kept in a network of *peers*. The larger the network, the more robust it will be, but it also will be correspondingly slower. This decentralised architecture that marks blockchains adds to their security. This effect is strongest in public blockchains, such as cryptocurrencies. These are freely accessible networks with millions of members. For smaller applications, such as supply chains or smart contracts, this may be too large. In that case, a *federated* or a *consortium* blockchain solution may provide better control and speed as a smaller number of nodes is deployed. Private blockchains leave most of the decentralised architecture intact[60]. The way blockchain technology works influences the confidentiality, integrity and availability of the blockchain and the data it contains.

[54] https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-blockchain-risk-management.pdf

[55] https://www.bbc.com/news/world-us-canada-47123371

[56] https://en.wikipedia.org/wiki/Cryptographic_hash_function

[57] https://www.coindesk.com/bitcoin-bug-guide-transaction-malleability/

[58] https://en.wikipedia.org/wiki/Merkle_tree

[59] https://allesovercrypto.nl/article/consensus-algoritme-welke-zijn

[60] https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/

Confidentiality

"Confidentiality supports the principle of 'least privilege' by ensuring that only authorised individuals, processes, or systems should have access to information on a need-to-know basis."[6162] Blockchain technology was never designed to provide confidentiality. On the contrary, the basic concept is that the information should be public, reducible to a source and integral![63] When an attacker gains access to the blockchain, he gains access to the data. This is why authentication and authorisation *controls* must be put in place.

Nowadays, implementations that support confidentiality by automatically encrypting the entire block are available.[64] This protects the blockchain transactions against unwanted perusal during transport. This is especially important for *permissioned*, *federated, and private blockchains*. It is best not to depend just on the security measures employed by most responsible organisations (firewalls, network segmentation, IDS/IPS, etc.). These are not always sufficient. Information security best-practice dictates that the application itself should be designed with built-in security. In case of (unauthorised) access to the network, the application is both the first and the last line of defence.

To protect content, blockchain alone is insufficient. A block has a limited size. Hence, blockchain is most suitable for a very robust financial application, with large amounts of transactional data and few documents. It cannot hold large (numbers of) documents[65]. These will have to be encrypted and stored elsewhere. The corresponding key material can be stored in a transaction, thus using the blockchain to protect the key material.

The Ethereum blockchain may serve to illustrate this. It is commonly used for smart contracts. A normal contract describes the terms of a relationship. In a smart contract, the relationship is digitally defined in an application. The transactions executed by the application are stored in the blockchain. Even file-sharing applications based on blockchain are available.[66] This technology is destined for major advances in the future. Blockchain alone, however, will only play a supportive role in keeping documents confidential. The documents themselves need to be protected outside the blockchain.

A node in the blockchain performs and validates transactions using the private key. This is the digital *wallet*. As stated above, when this key is lost or stolen the contents of the wallet are lost to the owner. It is therefore vital to not only have a working backup of the private key, but also to protect both production and backup keys from unwanted access.

Cryptography alone cannot offer a solution. The physical security of the keys must be taken into account as well. After all, the value of the key equals the value of the blockchain. Several organisations provide guidelines for key management[67] and their use increases the security of the blockchain.

Integrity

Integrity in this context is the characteristic that information and systems are accurate and reliable and that unauthorised modifications are prevented.[68] Blockchains were designed to guarantee two

[61] (ISC)2. (2015). *Official (ISC)2 Guide to the CISSP CBK (fourth edition).* Boca, Raton, London, New York: CRC Press.

[62] https://www.nist.gov/publications/glossary-key-information-security-terms-1

[63] http://historyofbitcoin.org/

[64] https://media.readthedocs.org/pdf/hyperledger-fabric/latest/hyperledger-fabric.pdf

[65] https://www.coindesk.com/what-is-the-bitcoin-block-size-debate-and-why-does-it-matter/

[66] https://library.wur.nl/WebQuery/wurpubs/fulltext/425727;

https://storro.com/

[67] https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-57pt1r4.pdf

[68] (ISC)2. (2015). *Official (ISC)2 Guide to the CISSP CBK (fourth edition).* Boca, Raton, London, New York: CRC Press.

characteristics of integrity: immutability and non-repudiation.[69] As described earlier, advanced cryptography guarantees the intrinsic integrity of a blockchain transaction. Users certify their transactions with a digital signature. If the contents of a transaction change, the signature becomes invalid. This makes any transaction immutable. The group of transactions is protected by the Merkle Tree: any change in the tree changes the Merkle Root and renders the entire block invalid. A change in the blockchain (*fork*) requires 51 percent consensus that the new value is correct[70]. The more nodes in the network, the less the chance that malicious intentions will invoke this situation.

All transactions are certified by the user and validated by the network. The blockchain does not throw away any transactions. This means that any transaction is traceable to an identity. Every transaction is therefore connected to a known user. *While the blockchain grows, the assurance that the stored history is correct also grows*. This property provides an important information security attribute: traceability or *non-repudiation*[71]. The principle of consensus also adds to the integrity of blockchains. As long as less than 51 percent of the nodes in the network can be collectively manipulated for the same purpose, there is little danger of data changes taking place in the blocks.

Blockchain technology validates and protects transactions and input from the moment they are offered to the ledger. There is no guarantee that the offered transaction is valid. The blockchain is as secure as its sources. Here too, *garbage in = garbage out.*[72]

One of the greatest threats to blockchains is the *51 percent attack*[73]. When a single entity controls the majority of the *mining hash rate*[74], it has full control over the blockchain. The formation of *mining pools* increases this risk. Bitcoin actually experienced *majority power*[75].

The theoretical possibility of tracing blockchain transactions says nothing about the feasibility or the costs involved. Many cybercriminals like to be paid in bitcoin. It is difficult to detect and prevent bitcoin from being whitewashed. Knowledge and legislation are still lagging behind the modern means of transferring criminal money into the upper world[76].

Blockchains can only get bigger. Every transaction remains present. If the transactional data contains personal data, this might be in violation of GDPR. It would be wise to assess the privacy challenges and possible solutions prior to implementation.

Availability

Availability means: "reliable and timely access to information and resources for authorised individuals or processes"[77]. Availability is not obvious. Cyberattacks that target the availability of services or data are all too common. DDoS attacks (Distributed Denial of Service) are a well-known example. These disrupt internet services and block applications. The cost and social risk of DDoS will increase over the coming years[78].

The decentralised architecture makes blockchains less sensitive to DDoS attacks. A DDoS attack on a blockchain demands that a large number of targets are hit simultaneously. This was proven in 2014

[69] https://www.yjolt.org/sites/default/files/shackelford19yjolt334_0.pdf

[70] https://hackernoon.com/what-is-a-51-attack-or-double-spend-attack-aa108db63474

[71] (ISC)2. (2015). *Official (ISC)2 Guide to the CISSP CBK (fourth edition).* Boca, Raton, London, New York: CRC Press.

[72] https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Technology/IE_C_BlockchainandCyberPOV_0417.pdf

[73] https://www.investopedia.com/terms/1/51-attack.asp

[74] https://www.uitlegblockchain.nl/hashrate/

[75] https://www.coindesk.com/eba-51-attack-remains-bitcoins-biggest-problem/

[76] https://openaccess.leidenuniv.nl/bitstream/handle/1887/62424/Bijdrage_Custers_Strafblad.pdf?sequence=1

[77] (ISC)2. (2015). *Official (ISC)2 Guide to the CISSP CBK (fourth edition).* Boca, Raton, London, New York: CRC Press

[78] https://www.zdnet.com/article/ddos-attacks-getting-bigger-and-more-dangerous-all-the-time/

when Bitcoin survived a DDoS attack[79]. However, in 2016 the Ethereum blockchain fell victim to a DDoS attack that targeted the internal workings of the client[80]. Eventually, a new set of rules was needed to stop the attack.[81]

A second well-known problem is *Transaction Malleability*. The transaction identifier is changed before the transaction is added to the blockchain. This renders the transaction invalid[82]. The proof-of-work principle requires the node to solve a difficult puzzle. Consequently, it may take some time to anchor the transaction to the blockchain. For Bitcoin, the processing time averages ten minutes[83].

Blockchains lack a s*ingle point of failure*, making the network resilient against the failure of one or multiple nodes. The remaining participants have access to all data and can continue working. Problems will only occur when a large number of nodes is taken down. The best-known blockchain platform, Bitcoin, has resisted several attacks during its ten-year existence.[84] However, the increasing number of applications will also expand the possibility of incidents. The resilience of the blockchain therefore requires constant attention.

Conclusions

Blockchains use proven technology – cryptography, distribution – in a new way and are highly available by design. The data in the blocks is immutable. The correctness and origin are traceable up to the first block in the chain. *The system integrity of blockchains is excellent*. Blockchains were not primarily designed to keep their content confidential. This does not necessarily imply that the technique is unsuitable for confidential information, although additional measures are required to ensure confidentiality.

Points for attention

- Blockchain is not a solution for every IT application. However, it ensures very secure transaction processing when the following four factors occur in combination:
    1. "A group of people or multiple parties frequently generate transactions that are dependent on a third party.
    2. The third party cannot be trusted and/or the authenticity of the transactions is questionable.
    3. The validation of transactions is a priority, so the presence of an enhanced system that renders data authenticity and integrity is important.
    4. Data integrity over confidentiality and processing performance is important. For time-sensitive applications, the blockchain is not appropriate as it takes time for a block to be accepted in the chain"[85].

[79] https://www.forbes.com/sites/coindesk/2014/03/04/bitcoin-whatever-doesnt-kill-it-only-makes-it-stronger/#b145d1e71f22

[80] https://blog.ethereum.org/2016/09/22/ethereum-network-currently-undergoing-dos-attack/

[81] https://www.coindesk.com/ethereum-fourth-hard-fork-stop-blockchain-attacks/

[82] https://bitcointechtalk.com/transaction-malleability-explained-b7e240236fc7

[83] https://www.researchgate.net/profile/Saraju_Mohanty/publication/323491592_The_Blockchain_as_a_Decentralized_Security_Framework_Future_Directions/links/5aa202e5aca272d448b4c297/The-Blockchain-as-a-Decentralized-Security-Framework-Future-Directions.pdf

[84] http://historyofbitcoin.org/

[85] https://www.researchgate.net/profile/Saraju_Mohanty/publication/323491592_The_Blockchain_as_a_Decentralized_Security_Framework_Future_Directions/links/5aa202e5aca272d448b4c297/The-Blockchain-as-a-Decentralized-Security-Framework-Future-Directions.pdf

- The greatest risk when using blockchains is the management of the *private keys*. These provide access to the network, the transactions and the data in the chain. Special measures must be taken to prevent the private key from falling into the wrong hands or from being destroyed.

5 Smart contracts; how smart really?

Natascha van Duuren

In 1994, US lawyer and computer scientist Nick Szabo introduced the concept of a 'smart contract'. In this kind of contract, the agreements between the parties are not laid down on paper, but in another form, specifically a computer program. By documenting a set of agreements in code in a blockchain, it is theoretically possible to set up a contract that is guaranteed to perform itself, without any of the contract parties being able to commit breach of contract[86] and, incidentally, also without a third party (such as a civil-law notary, bank or insurance intermediary) being required. Twenty-five years after Szabo and this special ICT application is still coming up against legal obstacles, for the time being. Its practical use could nonetheless be possible and useful, however, depending on the subject and nature of the contract.

Introduction

A distinction can be made in smart contracts between determinist and non-determinist versions. In the first situation, the network itself has sufficient information to perform the smart contract entirely. In the case of a non-determinist smart contract, an external source is needed (oracle) to provide the network with the necessary information from the 'real world' so that the agreements can be performed. For instance, this could be up-to-date exchange rate information or information on whether certain conditions have been fulfilled.

The Ethereum blockchain is an example of a public blockchain specifically designed to support smart contracts.[87] It is relatively simple to build smart contracts within the Ethereum network using the Solidity programming language, a programming language that displays agreements with the well-known JavaScript. The advantages are also clear. The smart contract is accurate, reliable, efficient, inexpensive, no intermediary is required *and* - last but not least - it is guaranteed that the contracts will be performed in the agreed manner. Smart contracts can look forward to a brilliant future, therefore. Or are there clouds on the horizon?

All sorts of possibilities

Smart contracts can be used in different ways. It is conceivable, for instance, that such a construction could be used for (just) the *execution* of certain components of an agreement. The parties conclude a traditional (written) contract. Certain agreements are then translated into computer code and the code is subsequently performed on the blockchain. The advantage of using smart contracts in this way is that for matters concerning the establishment and interpretation of the agreement, the tenets of the law of obligations familiar to us from the current Dutch Civil Code can 'simply' be tied in with.

There is the risk, however, of a discrepancy between the agreements on paper, on the one hand, and the content of the code, on the other. In order to prevent this risk, there will have to be close

[86] For a detailed discussion of the nature of the smart contract, see K. Werbach & N. Cornell, *Contracts Ex Machina*, 67 Duke Law Journal 2017, p. 6-8, 24.

[87] https://www.ethereum.org/. One example of a private blockchain that can support smart contracts is Clearmatics, https://www.clearmatics.com/.

cooperation between the lawyer who drafts the contract and the person who subsequently programs the agreements.

Another possibility is that the smart contract could be used to *fully* codify the traditional written contract. The advantage of this kind of use is, in any event, that there can be no discrepancy between the written and programmed agreements. This does put people in *terra incognita*, however, when it comes to contract law. A contract established electronically is, after all, only equated with a written contract if a number of conditions are satisfied.[88] One of these conditions is that the contract must be able to be viewed by the parties.[89] The question is whether publication of the source code (of a blockchain) is sufficient to satisfy this requirement.

Since here, too, the technology is ahead of the legislation, the answer to this question is still unanswered for the time being in the Netherlands. In a number of US states, the legislator has already taken the position that a smart contract cannot be denied any 'legal effect, validity or enforceability' simply because it is a smart contract.[90] Here is a task for the Dutch legislator, therefore, if it likewise wants to anticipate in a timely manner the rise of smart contracts as a specific application for blockchain technology.

A *Ricardian contract* - which can be read by both virtual machines and by people[91] - could, for the rest, present a solution for the time being, both for the risk of discrepancies between the agreements on paper and the programmed agreements, and for the uncertainty of whether the requirement that the contract can be viewed by the parties is satisfied.

Not a full replacement

For the time being, it is not imaginable that smart contracts will replace all traditional contracts in the near future. After all, computer language is an instructional language. The type of clause that a smart contract can handle well is the kind that reads: 'if A happens, do B.' Many traditional contracts are full of passive and/or vague concepts, however. The parties commit to work together 'in all reasonableness', for instance, or to take 'appropriate measures'. Contracting parties use these terms because it is often simply not possible to write out all the possible situations or scenarios in advance in concrete wording in a contract. It is therefore expected to be difficult to fully and exclusively translate traditional contracts into or replace them with smart contracts and *hybrid versions* will mainly be used for the time being.

Service level agreement

Smart contracts are often mentioned in relation to mortgages, insurance policies, copyrights and music rights and the contracts in the property sector. A type of contract that is hardly mentioned in the context of smart contracts, if at all, is the SLA. Even though an SLA seems ideally suited for integration as a smart contract within an agreement. The data needed to measure a certain service level can often be logged automatically. For instance, the number of seconds within which a telephone call must be answered.

---

[88] Article 6:227a DCC, Article 3:15a DCC and Article 156a DCCP

[89] For a discussion on smart contracts and statutory requirements for the establishment of a contract under Dutch law, see the Smart Contract Working Group of the Dutch Blockchain Coalition, 'Smart contracts als specifieke toepassing van de blockchain-technologie' [Smart contracts as a specific application of blockchain technology], www.dutchblockchaincoalition.org, p. 23-29.

[90] See, for instance, Senate Bill 1662 of the State of Tennessee http://www.capitol.tn.gov/Bills/110/Bill/SB1662.pdf: '*No contract relating to a transaction shall be denied legal effect, validity, or enforceability solely because that contract contains a smart contract term*'

[91] *A Ricardian Contract can be defined as a single document that is a) a contract offered by an issuer to holders, b) for a valuable right held by holders, and managed by the issuer, c) easily readable by people (like a contract on paper), d) readable by programs (parsable like a database), e) digitally signed, f) carries the key and server information, and g) allied with a unique and secure identifier.* See https://nakomotoinstitute.org/the-ricardian-contract

Using these data, a smart contract can assess whether the relevant service level has been achieved and a bonus/malus can be incorporated in the monthly invoice automatically.

For the rest, it is to be expected that the domain of application for smart contracts will grow the more mature the technology behind blockchain becomes and the more processes in society become digitalised. Furthermore, the blockchain fits in well with the increasing shift towards a sharing economy. A number of big companies, including Microsoft, Samsung, JP Morgan and BP, joined the Enterprise Ethereum Alliance (EEA) in February 2017.[92] This collaboration wants to use open standards and knowledge sharing to investigate how the adoption of Ethereum blockchain technology by businesses can be accelerated and, for example, '*the solutions that will be the foundations for business going forward*.'

Computer says 'pay'

A special point of attention is the rigidity with which the programmed code will be executed. Imagine that a smart contract emerges to do something very differently from expected or the smart contract has been poorly programmed by the developer. The contract parties may want to reverse transactions in that case. Performance already provided may also have to be reversed if the oracle has supplied inaccurate information, the content of the smart contract is in contravention of mandatory law or if one of the contract parties invokes error. This requires changes to the code, but that is not necessarily possible. In fact, the unalterability of the data is precisely one of the special features of blockchain.

It is good to have some perspective, however. First of all, it is often still possible to change the code; the majority of the blockchain participants just have to agree to that.[93] That will take some doing, of course, even aside from the fact that it is a somewhat controversial procedure. Secondly, there is an option of programming the code so that there is room for human intervention in the performance of the agreements. Some even argue that a 'kill switch' should be made mandatory, a functionality that makes it possible to stop the performance of a smart contract in certain circumstances.[94]

Cryptocurrency instead of euro

Most of the contracts created for the B2B market use euros (or in some cases, dollars) as consideration. Supplier A supplies a product or service to customer B. Customer B must pay a sum of money as consideration. To date, smart contracts only allow the use of cryptocoins or tokens. The Ether token (ETH) is used in the Ethereum blockchain, for instance. The use of cryptocurrencies is not without risks, however. De Nederlandsche Bank points to the risks related to the absence of both supervision, a guarantee system and a responsible party which offers recourse.[95]

Added to this is the fact that the legal status of cryptocurrencies is not yet entirely clear. The District Court of Overijssel ruled, for instance, that a cryptocurrency like Bitcoin cannot be considered

[92] https://entethalliance.org

[93] The crowdfunding platform The DAO was launched on the Ethereum blockchain in April 2016. A few weeks after the launch, a weakness in the software was exploited by a participant who managed to entirely empty the portfolio of several investors. Reversing the transactions required changes to the original code. The majority of the participants ultimately agreed to this. Some of the participants refused to comply with this and the Ethereum blockchain split into two communities. On the DAO hack, see T.J. de Graaf, *Van oud naar nieuw: van internet naar smart contracts en van mensen naar code [From old to new: from internet to smart contracts and from people to code]*, WPNR 7199-7200; T.F.E. Tjong Tjin Tai, *Smart contracts en het recht [Smart contracts and the law]*, NJB 2017/146.

[94] See J.B. Schmaal and E.M. van Genuchten, *Smart contract en de Haviltex-norm [Smart contract and the Haviltex standard]*, Tijdschrift voor internetrecht [Journal for internet law] no. 1 March 2017, p. 15.

[95] Position Paper from De Nederlandsche Bank, Round-table discussion on Cryptocurrencies/ICOs, 24 January 2018.

money in the sense of Part 6.1.11 of the Dutch Civil Code, but must be seen as a means of exchange.[96] Last but not least, parties in the B2B market will still want 'real money' as consideration for the time being. This is the reason that it seems that the use of smart contracts will not take off for a large number of transactions in the business market quite yet.

Points for attention

- By definition, a smart contract is neither 'smart' nor a 'contract' in the legal sense. It is a computer program that is executed ('runs') on a blockchain.

- The Ethereum network is often mentioned in the same breath as smart contracts. Since this is a public blockchain, however, this network is less suitable for smart contracts in B2B relations where companies do not usually want to make their transactions public. Smart contracts will therefore mainly play a role in private blockchains.

- The qualification and enforcement of smart contracts raises new legal questions. Until this uncertainty has disappeared, it is wise to use a hybrid form: the smart contract *in supplement to a traditional contract*. If the parties wish to work exclusively with agreements in code language and want to accept the outcomes of that in advance, it is advisable to document this intention explicitly and in writing.

- The smart contract is most suitable for contract relations that lend themselves to translation into computer language. Deliverables must be able to be described precisely and verified digitally and objectively. The smart contract is less suitable for contract relations that must be flexible and where the contract content still needs to be amended in the interim.

- The quality of a smart contract is contingent on the quality of the developer, the chosen programming language, blockchain technology and - if applicable - the oracle.[97] This means that when using smart contracts, while contract parties may no longer be dependent on an intermediary, new dependencies do arise and there must be trust in these parties.

[96] District Court of Overijssel, 14 May 2014, ECLI:NL:RBOVE:2014:2667

[97] On the reliability of the oracle, see: www.coindesk.com/mit-testing-smart-contract-powered-bitcoin-lightning-network.

6 Healthcare sector and blockchain: a solution looking for an application?

Dirk de Wit

Whether it concerns the exchange of data inside institutions or between hospitals, or communication between hospitals and general practitioners, we are facing huge challenges in the area of digital data exchange. The current practice is vulnerable to mistakes in manual transfer, while the administrative burden for the professional is also a recurring theme. The problem is not new and not limited to the Netherlands. Since the failure of the nationwide introduction of a platform for the exchange of electronic patient records (EPDs) in 2011, various initiatives have been developed to improve information flows in healthcare: the internationally acknowledged struggle to achieve interoperability. Which is why new developments, such as blockchain and artificial intelligence, are attracting so much attention. Certainly when the initial ideas about using blockchain in healthcare emerged, there was a strong feeling that it would help with the exchange of digital data. Blockchain was seen as an alternative to electronic patient records that could give patients control over their own health data.[98] The same idea is reflected in the development of the personal health environment. Here, too, there is great confidence that the digital exchange of data between care providers and patients will significantly improve. After all, patients will have more control over their personal data. The question of whether blockchain technology has this transformative potential is an important one. Will it live up to the promise of liberating healthcare that was expected in 2016 and 2017?

Developments over the past two years

In a way, it still too early to draw conclusions. Two years ago, the first conference on blockchain in healthcare was held in the Netherlands, with participants from patients' associations, digital security experts and ICT managers from hospitals. The question mark in the presentation title 'Healthcare unchained with blockchain?' was there for a reason.[99] The new digital technology was then primarily perceived as *a promise* for the healthcare sector because practical applications were still lacking. The practical examples of blockchain that were available came from the financial sector in the shape of cryptocurrencies.

A rare example of an initiative from the care domain that attracted attention was a *proof of concept* for the provision of a medication overview, carried out by the Reshape Centre of the Radboud UMC. 'Patients decide with which care providers they want to share their medication overview and to which pharmacist they want to send their medication prescription'.[100] It should come as no surprise that this trial focused on the medical prescription of medicines (medication). This 'medication safety'

[98] John D. Halamka, MD, Andrew Lippman, Ariel Ekblaw, The Potential for Blockchain to Transform Electronic Health Records, in Harvard Business Review, March 3, 2017.

[99] Frederieke Jacobs, *De zorg ontketent met blockchain?*, included in https://www.smarthealth.nl/trendition/2016/07/07/blockchain-zorg-congres/

[100] Idem

continues to be an ongoing and complex challenge in the health sector. Approximately 25,000 preventable admissions take place in the Netherlands every year as a result of using the wrong medicines (or the wrong dosages). The use of blockchain technology provides transparency about which healthcare provider has prescribed which medicines and can clearly show which medication the patient is actually using. The Reshape Centre's promise, however, was accompanied by warnings about the strict regulations in the healthcare sector and the timing of this technology. Blockchain technology is still at an early stage in the hype cycle.

Research

The focus on blockchain in the health sector has since continued in both pilots and reports. For example, in 2017 the Dutch expertise centre eHealth Nictiz published a balanced report on the possibilities and risks related to blockchain. The report indicates that blockchain offers a promise in healthcare. Yet it is not seen as a solution to the major issues in the field of digital data exchange, especially in terms of cross-sector information exchange.[101] It is a young technology whose value for the health sector can only be discovered through pilots and experiments.

Nictiz believes that the greatest opportunity provided by blockchain is that it can give patients control over their own data. But does the average citizen want this type of control? In addition, the experiments can help the sector see how far the possibilities of this technology actually extend. The snapshot of blockchain in healthcare leaves nothing to be desired. According to the expertise centre, there is an imaginary hammer for an imaginary nail.

Experiments

Trials have already been performed at various locations. One good example involves a pilot that the Netherlands Care Institute (ZIN) carried out in the field of maternity care.[102] Using blockchain technology, maternity nurses and young mothers updated the time registration on their smartphones. In this way, the mothers gain an insight into the number of maternity care hours they still have. ZIN concluded that the participating parties endorsed the added value of blockchain sufficiently to recommend further research. For healthcare, the institute is currently arguing for the use of a *permissioned (private) blockchain*: this means that the partners in the blockchain are always known because access to the system is only granted with permission.[103]

Interestingly, the institute draws attention to the need to agree on cooperation in order to clarify roles and engender trust between the parties. ZIN also states that it is still unclear how blockchain relates to the new rules for processing personal data as laid down in the General Data Protection Regulation (AVG), which came into force on 25 May 2018. For example, it gives rise to questions about the new right to be forgotten and about the subject of the exchange of medical personal data between different sectoral information systems. It is still a technology in its infancy in which the rules are not clear. At least, not yet.

[101] Jaco van Duivenboden en Maarten Ligtvoet, *Blockchain in de zorg*, Nictiz, 2017.

[102] Idius Felix, Maarten Nap, Marleen Nuijten, Eva Piller, *Praktijkproef blockchain kraamzorg met Mijn Zorg Log*, Rapportage (ZIN, 14 juni 2018), https://www.zorginstituutnederland.nl/publicaties/rapport/2018/06/14/praktijkproef-blockchain-kraamzorg-met-mijn-zorg-log.

[103] In a *permissionless* (open - public) model, nothing has been determined about who can add blocks to the chain (everyone can mine new blocks). In a *permissioned* (closed - private) model, it is precisely recorded who these *miners* are.

Solution to serious exchange issues?

New technology creates new images. It takes some time before a shared understanding and meaning arises. In mid-2017, Zorgvisie published a call for healthcare to respond to blockchain because the technology can reduce the administrative burden.[104] More recently, articles have appeared stating that the issue should be looked into more fundamentally. Some parties assume that healthcare essentially differs from other sectors to such an extent that blockchain will not be a serious 'disruptor' in this industry.[105] So no health sector disruption, but a fairy tale for believers. There are three arguments to support this hypothesis. In the healthcare sector:

- It is about patients, operations, treatments and medicines. Digital data exchange is a consequence of these functions and only sometimes a necessity.
- Most of the data is stored in (non-central) electronic patient records (EPDs), which prevent open data exchange.
- The reliability of the personal data is a derived problem. The problem is often not related to fraudulent actions but to the absence of reliable, up-to-date information or unauthorised access. For example, is the prescribed use of medication equal to its actual use?

We believe that the opportunities for blockchain technology will primarily involve support processes such as claims for expenses and patient permissions (administrative) rather than primary processes dealing with patients and treatments.

Conclusions

The introduction of a new technology is generally accompanied by enthusiasm and potential, often followed by disappointment after the first practical experiences: Gartner's phase of disillusion. Blockchain in the health sector is currently balanced between the two. We have the believers and the sceptics.[106] There is a rumour that the blockchain hype is over. *What will happen after the hype?* Whatever the case, the use of blockchain does not appear to be high on the agenda of the CIOs of hospitals in the Netherlands. For the time being, it continues to be a promise with potential. According to McKinsey, the health sector may be one of three sectors in which the business value of blockchain can generate huge revenues (along with the financial sector and the government) precisely because the availability of data through the 'value chain' can be organised more effectively.[107]

Experiments in the United States have led to MedRec (www.medrec.io), which is a data platform on which patients and professionals play a central role. The Dutch program that stimulates the development of a Personal Health Environment, MedMij, consciously does not use blockchain because it is not yet a proven technology.[108] The use of blockchain certainly offers potential to strengthen the control and coordination of the citizen/patient, as shown by MedRec.

Nevertheless, I don't expect the health sector to eagerly embrace blockchain technology and unchain digital data exchange any time soon. *At this stage, it is still a technology looking for a good application*. McKinsey also says that the technology is actually too immature. Here, too, there are no

[104] *Oproep aan de zorg: gebruik Blockchain*, Zorgvisie 23 juli 2017

[105] Mark de Graauw, *Blockchain in de zorg is grootste hype sinds uitvinding van Internet*, https://www.smarthealth.nl/2018/01/10/blog-blockchain-zorg-hype/

[106] For example, see for some scepticism: Jesse Frederik, *Blockchain, a solution for almost nothing* (translated) (De correspondent, 25 August 2018), https://decorrespondent.nl/8628/de-blockchain-een-lossing-voor-bijna-niets/519071687772 -2a5ee060.

[107] Brant Carson, Giulio Romanelli, Patricia Walsh, and Askhat Zhumaev, *Blockchain beyond the hype: What is the strategic business value?* (McKinsey, June 2018)

[108] See: www.medmij.nl

standards or regulations and the danger of silo-blockchain focused on specific applications is around the corner. It also sees potential in the field of insurance and payments. The value and liberating nature of blockchain may yet prove itself over the next five years.

It is only through experimentation and learning that we can ultimately achieve clarity about whether (open or closed) blockchain technology can be used meaningfully in healthcare. Only then will we know the answer to the question of whether blockchain is the metaphorical hammer or the nail.

Points for attention

- The IDC research agency expects blockchain to emerge from the experimental phase in a healthcare perspective by 2020 at the earliest. This digital technology can offer a practical solution to help improve digital data exchange in multiple patient information systems. However, we do not know in which sub-domain the concrete applications will take place.

- Unlike blockchain applications in other sectors, digital data exchange in healthcare is elementary but secondary to the primary process of treatment. The technology must have proven itself before the healthcare system will use it.

- The application of blockchain in the health sector focuses on specific areas in which patients/citizens and healthcare professionals interact or in which health care professionals want to reach mutual agreement. The connection to an 'Electronic Health Record' is interesting and should be further investigated.

- New technology – if it is not medical technology – is not readily accepted in healthcare. That certainly also applies to blockchain technology, which is after all difficult to grasp. The value must be experienced by healthcare professionals and patients/citizens in practice.

7 Blockchain in the payment system

Marnix Blom

The bitcoin blockchain shows us that transfer of the ownership of digital assets can be achieved in a fully distributed architecture. The traditional role of banks as the central party in a transaction where the payer and payee both rely on third parties to validate their transaction is then disintermediated. That is nothing less than revolutionary.
Which consequences can we expect from this academic insight in practice? Will this lead to the transformation of the payment system in order to adopt a distributed architecture? Which arguments lead to that conclusion? Or is demonstrating that the possibility in itself is not sufficient to influence practical reality? The Dutch Payments Association delved into this with a number of its members.

Cash, but then in a digital form

Blockchain mainly derives its fame from bitcoin. Bitcoin shows us that transactions in bearer assets can be successfully modelled in a digital environment without requiring a central authority to prevent double spending. With physical cash, it goes without saying that a payer no longer controls the bills and coins he hands to a recipient when making a payment. In the digital world, however, that simple transaction is difficult to model. Digital assets that a payer sends to a recipient continue to be the in payer's possession . Now only a third party can decide which party can call itself the owner of the digital asset. This places the third party in a particularly powerful position; the payer and the payee are in fact entirely dependent on this party for an assessment of who actually owns the asset.

The infrastructure of the current scriptural payment system is based entirely on this reality: the bank has the final say about the balance that account holders hold there. Between banks, it is ultimately the settlement infrastructure of the European Central Banks, Target2, that determines which balance is owned by whom. In order to ensure that all this is done fairly and reliably, the payment system therefore largely consists of control overhead that continually audits the stream of transactions, monitors the integrity of the software used and supervises the execution of procedures.

Bitcoin shows that the process of accounting for the ownership of digital assets can also be carried out in a fully distributed fashion, with no concentration of power.

Removing power concentrations from the infrastructure

Internal controls, auditing, supervision: in a distributed setup, risks originating from power concentrations in the infrastructure are eliminated. This make it possible to eliminate all kinds of control tasks and costs. For payments, this is what makes a distributed blockchain infrastructure attractive.
An interbank study by banks and the Dutch Payments Association into the feasibility and usability of such a distributed payment infrastructure shows that the ideal of a self-monitoring infrastructure without power concentrations has a number of drawbacks. The main drawbacks are the problematic switch from the existing paradigm to a blockchain infrastructure and the lack of urgency in making such a change.

Two paradigms at the same time?

Both the existing design of the payment system and the distributed design derived from blockchain are conceivable. However, a combination of the two paradigms is problematic. The world of payment transactions enabled by third parties can be linked with a distributed infrastructure without power concentrations in two ways. But each has its own drawbacks.

One central party can take care of the interface, resulting in a concentration of power. We know this model from the link between the scriptural 'giro' payments infrastructure (transactions enabled by third parties) and the world of cash (where transactions are carried out in a distributed way). Here the Central Bank supplies the interfacing and is in fact the only party that can fulfil this role. The Central Bank guarantees the constant exchangeability of scriptural and cash euros at an exchange rate of 1 to 1. This is a special role with far-reaching consequences.

The unlimited and risk-free interchangeability of scriptural money and cash means, among other things, that central bank interest on scriptural money cannot fall below 0%. After all, cash has an intrinsic interest of 0%. With a substantial negative interest rate on scriptural balances, all value will flow to cash. This limits monetary authorities in their interest policies, known as the Zero Lower Bound. Making a risk-free connection between assets on a blockchain-based payment infrastructure and the existing giro infrastructure could, as it is for cash, also be provided for by the central bank. Unlike cash, an interest rate can be set for digital central bank money on the blockchain. The phenomenon is called the Central Bank Digital Currency[109], an interesting monetary field of science that has already been widely publicised.[110] However, for each currency there is only one entity that can determine its introduction. For the euro, that is the European Central Bank.

The alternative has far fewer dependencies. Market parties can themselves also maintain an interface between the traditional money infrastructure with third parties and the new distributed money infrastructure. This will lead to fluctuating exchange rates between assets in the two systems. This is the world of euros and bitcoin. Or euros and dollars, for that matter. The feasibility of this approach has been proven, but the disadvantages are also well-known: exchange rate fluctuations. For general use, it does not look like there are advantages that outweigh this disadvantage. Because, what would actually be the advantage of a blockchain-based payment system? And who stands to benefit from these advantages?

Possible benefits

Cost?

A blockchain-based payment system would eliminate a great deal of control overhead, resulting in efficiency gains. This could lead to lower tariffs for the users of the payment system due to a lower cost price. What do we mean exactly? The costs for the payment infrastructure will certainly not drop to zero, nor will the prices for end users (there is more to do than just keeping records – for example, fraud detection, money laundering checks, customer service, etc.).

The order of magnitude of the possible price reduction is therefore limited to a few cents per transaction. The bottom line efficiency gain for the infrastructure therefore only adds up to serious amounts in the case of very large numbers. This makes the development of such an efficient payment infrastructure unattractive compared to infrastructures where the costs per individual transaction are

[109] https://en.wikipedia.org/wiki/Central_Bank_Digital_Currency

[110] See the Wikipedia lemma: lemma https://en.wikipedia.org/wiki/Central_Bank_Digital_Currency voor diverse verwijzingen naar publicaties

considerably higher. The advantage simply increases faster with, for example, remittance (sending money to distant countries), trade financing or correspondent banking. The use of blockchain as a cost-reducing innovation is therefore more likely to develop in these areas.

Functionality?

Could blockchain help enrich the functionality of the payment system? From 2019, payment traffic will provide instant payments: 24x7x365 irrevocable payment (after full rollout) between all payment accounts within 5 seconds and (for the Netherlands) for all amounts.[111] The question here is which functional extensions are still conceivable. Micro payments, the Internet of Things (IoT) payments and conditional payments all come to mind. However, there are no good arguments for realising these applications within the payment infrastructure layer. The same functionality can be realised more effectively and with fewer dependencies in a separate layer.

Payment is defined as the settlement of debt. This only makes sense when a certain risk of non-payment must be covered. This does not apply to individual micro payments. The aggregation of multiple small transactions to one larger payment is the best solution.

In the case of the IoT, the assumption is that billions of entities could emerge with balances and a mandate for making payments. The existing infrastructure is not a priori unsuitable for this, as existing IBANs have up to 32 positions.[112] That offers space for more than one quintillion accounts. Furthermore, there is no compelling reason why IoT entities should all be represented individually (without aggregation) in the payment infrastructure with their own unique account number. Lastly, with conditional payments an associative connection with the term ‘smart contracts’ from the blockchain world can be established quickly. From the payment infrastructure perspective, however, conditional payments are very normal irrevocable payment transactions that have come about because (and after) certain conditions have been met.

The 'why' of these payments is not a part of the infrastructure, just as for all the other transactions in the payment infrastructure. All in all, it cannot be said that new and meaningful functional extensions to the payment infrastructure have come into play with blockchain.

Continuity?

The distributed design of blockchain is creating ultra-robust infrastructures that are almost impossible to eradicate. With the increasing societal importance of the payment infrastructure, this appears to be a good match. The question, however, is whether this continuity argument justifies a switch to the blockchain paradigm. In practice, the continuity of the current infrastructure is deemed to be sufficient. It is unclear to which extent a black swan event[113] such as a serious disruption of the payment infrastructure continuity could in itself constitute a sufficient reason for action.

Conclusion

Although blockchain presents an attractive new paradigm for a robust and efficient payment infrastructure with the opportunity for unprecedented freedom in monetary policy, the analysis shows that both the transition to such a system and the appraisal of any concrete benefits involve considerable

[111] See https://www.betaalvereniging.nl/betalingsverkeer/instant-payments/

[112] The structure of IBANs is laid down in ISO standard ISO 13616-1, the lenght of IBANs is determined per country and run up to 32 characters.

[113] Black swan: unexpected and disruptive event that no one saw coming or had predicting. The paradox is that in the current economic science the early detection of black swans is seen as the summit of risk management. (source: https://nl.wikipedia.org/wiki/Zwarte_zwaan_(economie))

obstacles. The momentum of blockchain therefore does not open up new avenues for improving the payment infrastructure. On the contrary, it prompts us to question the status quo and become involved in new experiments.

Insights

- If it can ever be demonstrated that blockchain technology can have a meaningful application in the payment system, this will certainly have to be preceded by the adoption of other blockchain domains where benefits accrue faster.

- Switching to a blockchain infrastructure may be feasible but is not necessary.

- The technical obstacles to realising a payment infrastructure based on blockchain are not dealt with here but have not yet been resolved.

- It cannot be ignored that blockchain has in any case demonstrated its influence on the momentum of infrastructural innovation and shown a general willingness to question existing architectures and processes. That alone is beneficial.

8 Trends in digital law: what about blockchain?

Victor de Pous

Over the past 25 years, a strong legislative offensive for digital technology and data processing has taken shape, which is currently growing in size, diversity and intensity. New regulation is coming from both the European Union and the Netherlands. Although the digital legal domain is much broader - think of intellectual property law, electronic commercial law and consumer law, for instance - two legal questions loom in the foreground: cybersecurity and privacy. These also touch on the construction and application of every peer-to-peer network that chronologically updates a mathematically encrypted and decentrally stored database. Neither the European Union nor the Netherlands currently has a *lex specialis* that applies generally or specifically to blockchain technology. Some countries, like the United States, do. In the meantime, the Dutch court has defined blockchain in decisions on several occasions.

Monumental codification

There is now so much digitally-related regulation in force in the Netherlands and Europe that the question of where to start is a logical one.[114] This area of the law is also constantly expanding. The starting point of the legislators is usually that special - therefore *deviating* - legal rules are needed for the development of the information society. This starting point leaves some room for negotiation.

First of all, (open) legal standards allow flexibility and can accommodate changes - also because modern regulations are often technology-independent by nature - unless substantive grounds prevent this in the concrete case. The fact that the adoption of ICT takes place partly, perhaps even largely, without any legal 'push', also plays a role. For instance, online shopping largely reached maturity because of its clear convenience and not thanks to a law that legalised electronic signatures.[115] It can also be advisable to allow a certain technology and its economic or societal applications to become entirely clear before formulating specific ground rules either per branch of industry or otherwise, also in a supplementary fashion.

For the rest, none of these analyses detract from the justified European desire to create a single internal digital market, which inevitably implies the harmonisation of legislation.

Other lines of development

The net around privacy protection is being pulled a bit tighter each time, in connection with *how personal data are handled*, for example with the widely known General Data Protection Regulation (GDPR). The special privacy regulations for sectors such as healthcare and education literally apply on top of this. We see the same - general and sectoral - approach in the various *network and information security regulations,* aimed at combating the wider problem of a lack of confidentiality in data processing.

---

[114] See for instance V.A. de Pous, *Recht op elektronische technologie 1983-2008 [Right to electronic technology 1983-2008]*, Amsterdam, 2008. From the same author, *Outlook digitaal recht 2019 – Wetgevingsspecial (preview) [Outlook on digital law 2019 - Legislation special (preview)]*, Amsterdam, 2018, for a selection of digital regulations taking effect, becoming applicable, being prepared or still on the drawing table in 2019.

[115] Or considered vice versa: countless individuals pay little heed to the prohibition against downloading music, films, software and games from illegal sources.

Another trend in regulation is the rise of *notification requirements for incidents* relating to digital technology and data processing**,** in the event of a security breach, loss of integrity or malfunction, for instance. Finally, the steady expansion of the legal *powers of supervisory authorities* is striking, including those of the Dutch Data Protection Authority and the Netherlands Authority for Consumers & Markets, as is the substantial increase in sanctions in the event of violations of a security regulation or notification requirement, for instance.

Blockchain regulation

A peek behind the scenes at various US states provides insight into the new regulation and policy intentions, but federal legislative bill H.R. 6913 focuses attention on more fundamental questions.[116] What is blockchain? The Blockchain Promotion Act of 2018 submitted in the House of Representatives on 26 September 2018 aims to bring stakeholders together in order to develop a common definition of blockchain. The next question concerns the US economy. Opportunities must be identified and innovation promoted, according to the draft bill. Legislation which is intended on the one hand to be a national, inwardly-focused marketing means and which on the other has a more substantive approach.[117]

We see the research line appearing on the west coast as well. On 28 September 2018, California's governor signed a legislative proposal prescribing that a government working group be set up. (Blockchain is defined here as: '*a mathematically secured, chronological, and decentralized ledger or database*.') Before 1 January 2022, the evaluations must be clear in relation to (i) the risks and benefits associated with the use of blockchain by government institutions and California-based businesses, (ii) the legal implications of the use of blockchain, and (iii) best practices for enabling blockchain technology to benefit the state, its businesses and residents.

Back to Washington DC. Harmonisation is a fitting means to combat the impending fragmentation by state. Blockchains need not be geographically limited, after all. On 2 June 2016, Vermont became the first state to grant blockchain-based files evidential weight in a court case. According to the Vermont Rules of Evidence, blockchain technology must be defined as: '*mathematically secured, chronological, and decentralized consensus ledger or database, whether maintained via Internet interaction, peer-to-peer network, or otherwise*'.[118]

The Arizona Commercial Code now defines the technology as: '*distributed ledger technology that uses a distributed, decentralized, shared and replicated ledger, which may be public or private, permissioned or permissionless, or driven by tokenized crypto economics or tokenless. The data on the ledger is protected with cryptography, is immutable and auditable and provides an uncensored truth*.'[119] As many legal definitions as there are states, it seems.

What then is provided for in blockchain legislation? A few topics. Arizona does not want lower regulators to involve themselves with blockchain, in the sense that a municipality may not prohibit or otherwise restrict an individual from running a '*node on blockchain technology*' at home. The legal standardisation of 'residential' use is an exclusive power of the state.[120] Other state legislation pertains to blockchain technology in the insurance legislation (California), while Delaware, for example, has rules in force which acknowledge the trade in shares via blockchain.[121]

---

[116] https://www.congress.gov/bill/115th-congress/house-bill/6913?q=%7B%22search%22%3A%5B%22H.R.+6913%22%5D%7D&r=1

[117] The latter aspect can also carry weight outside the national borders. The definition of cloud computing developed earlier by the US government is widely used internationally, for instance. https://csrc.nist.gov/publications/detail/sp/800-145/final

[118] https://law.justia.com/codes/vermont/2016/title-12/chapter-81/section-1913

[119] https://codes.findlaw.com/az/title-44-trade-and-commerce/az-rev-st-sect-44-7061.html

[120] https://www.azleg.gov/legtext/53leg/2R/laws/0208.pdf

[121] For an overview of state legislation, see: http://www.ncsl.org/research/financial-services-and-commerce/the-fundamentals-of-risk-management-and-insurance-viewed-through-the-lens-of-emerging-technology-webinar.aspx

Dutch case law

There is no blockchain law in the Netherlands, but there is case law to serve as a source of law. A search on Rechtspraak.nl for 'software*' on 12 October 2018 produced 3,647 judgments, rulings and individual decisions. 'Blockchain*' produces no more than 16 results. These virtually all relate to criminal law, in particular the crime of money laundering[122] using the cryptocurrency bitcoin, usually in relation to other crime, such as the drug trade or internet scams. There is one civil-law ruling which pertains to the dissolution of a purchase agreement in relation to bitcoins.

How does the Dutch court define a blockchain and what else does it say about it? A concise overview.

- *Criminal law*. According to the court, money laundering also covers all cases and all proprietary rights, including cryptocurrencies. 'After all, bitcoins are objects subject to human control with an economic value which is subject to transfer. They can be used for payment. They are also individually determinable: all bitcoins that have ever been mined and all transactions which are carried out using them are kept track of in the blockchain. The approach that a bitcoin is simply a series of numbers does not do justice to the economic reality' (District Court of Rotterdam on 30 May 2018).
- *Criminal law*. The court accepted the data contained in a block as evidence under criminal law and observed that the transfer of a bitcoin 'is registered in the "blockchain" (the data structure behind the bitcoin network) in which every transfer is registered' (District Court of Midden-Nederland on 22 January 2018).
- *Criminal law*. 'Cryptocurrency, such as the bitcoin, is digital money. The distribution of this money, the ledger, is kept track of in a decentralised network (the blockchain), a network of all users of this cryptocurrency that communicates using the internet. This kind of network is kept afloat by users and miners of the currency. Miners are users who use the computing power of their own computer to generate new crypto-money and to keep the cryptocurrency network operational' (District Court of Rotterdam on 22 December 2017).
- *Criminal law*. 'The technology behind the bitcoin is the blockchain, a kind of public archive or ledger of all bitcoin transactions. The blockchain visualises for every bitcoin, in chronological order, in which wallets it has been held' (District Court of Rotterdam on 8 November 2017).
- *Civil law*. '"Bitcoin" is the peer-to-peer network that is kept track of in a decentrally stored ledger - "the blockchain". A "bitcoin" is the digital coin that is sent via the Bitcoin network. The addresses to which bitcoins are sent consist of a unique series of numbers and letters. In the blockchain, an overview is kept of all addresses and transactions generated. The Bitcoin protocol is set up in such a way that miners (people who make computing power available in order to check the validity of transactions) can be rewarded with a number of bitcoins for their work in checking the validity of these transactions' (Appeal Court of Arnhem-Leeuwarden on 31 May 2016).

Conclusions

All sorts of legal rules standardise the construction and use of a blockchain application. Mandatory frameworks specific for digital matters consist, for instance, of regulations based on software copyright (right to error correction, right to create a back-up and right to interoperability) and 'cybersecurity' law (mainly security obligations and notification requirements). If the blockchain system processes personal data, then privacy law is added to this, involving, among other things, strong rights for data subjects and legal instructions in the form of privacy by design, including privacy by default requirements. There is no escaping it.

There is in principle no legal vacuum because a blockchain is part of our society, in which legal rules apply. The question does arise of whether special, therefore partially *deviating*, rules are desirable

[122] Article 420bis/420quater Criminal Code.

for the technology. As far as cryptocurrencies (as a property right) are concerned, from the cross-border abuse perspective, the Dutch government in any event finds this unavoidable, while the European Parliament is working on rules for 'initial coin offerings' (ICOs).[123] Much more specific legislation and regulations from the Netherlands or the European Union is probably not to be expected in the short term. We must not forget the activity of the court in interpreting law, of course.

Analyses

- The technological components of a blockchain are mainly computer programs or matters, such as the data structure and algorithm, laid down in software code. This is in any event subject to (software) copyright law and sometimes patent law as well. With regard to the development, delivery and maintenance of software - and more broadly: ICT systems - Dutch case law has a great many decisions. These can also relate to a blockchain project; public or private, permissionless or permissioned.

- Computer-generated evidence in various areas of the law (civil law, criminal law and, for instance, administrative law) has caused hardly any problems to date, as far as is known, under Dutch procedural law. Lines of source code, screenshots, print-outs (of an email), chat messages, telecommunication data, and more are usually accepted by both the parties and the court as evidence with a certain evidential weight, while this evidence is not in principle - or at least not by definition - *as irrefutable and traceable as the data recorded in a blockchain*.

- Special regulations for blockchains emerge to be at least twofold. They can have a restrictive effect to prevent undesirable behaviour. Or they involve legislation and regulation to encourage the technology by eliminating legal obstacles for a particular application, for instance, or to give a specific legal effect to data recorded in a blockchain, an effect which is currently lacking.

- For the time being, the European Commission and European Parliament are taking an extremely cautious approach, considering the fact that regulating too early could harm blockchain's potential. A parliamentary innovation group did draft a proposal for initial coin offerings (ICOs) to bring the issue of cryptocurrencies within the scope of a new European regulation for crowdfunding, which is currently being worked on.

- While the Netherlands wanted to create a favourable business climate for multinationals via the policy intentions to abolish dividend tax, which have since been withdrawn, EU member state Malta is opting for different kinds of measures for start-ups that work with blockchain technology, cryptocurrencies in particular. The Maltese parliament adopted three legislative proposals on 4 July 2018: the *Malta Digital Innovation Authority Act*, the *Innovative Technological Arrangement and Services Act* and the *Virtual Financial Asset Act*.[124] This is also legislation that serves as an outwardly-facing marketing instrument. '*While the blockchain sector in the rest of the world continues to operate in a legal vacuum, or, at best, a legal fog, Malta is leading the way as a crypto haven with a crystal clear legal framework for ICO regulation*.'

[123] https://www.the-blockchain.com/2018/09/06/european-parliamentarians-propose-eu-wide-ico-regulatory-framework/

[124] https://icomalta.com/ico-regulation/

9 Privacy and blockchain

Jeroen van Helden

The roots of modern privacy law stem from the 1970s and were developed when it became clear with what ease computer systems could store and further process large quantities of data. In essence, this important area of the law consists of a small collection of principles which have been taken over in the current General Data Protection Regulation (GDPR). They were deliberately formulated in a technologically neutral manner, do not refer to specific information technologies and were not drafted for a specific way of processing data. Paper files in the old-fashioned filing cabinet can also fall within their scope. And yet blockchain presents us with challenges. On the one hand, it presents a new and interesting data-processing model in which individuals have more control over their personal data. On the other hand, a number of special characteristics seem difficult to reconcile with the key principles of privacy law.[125]

Bottleneck 1: everyone sees everything

The technology behind blockchain makes it possible to synchronise distributed databases. A database that runs on a blockchain is not stored on a central computer or server, instead the files are located simultaneously on multiple computers, where the information is updated according to a consensus model. All the participants in the blockchain have a copy of the full database. In the event of the Bitcoin blockchain, this means that every user has insight into the entire transaction history of all the other wallets.

Privacy law requires that organisations only collect data for clearly described and legitimate purposes, that they not collect more data than is necessary for these purposes and that they secure these data appropriately. At the bank, I can therefore view my own transaction history, but not that of my neighbour. There is no need for that, and it is therefore not permitted. If the bank were to disclose my transaction history to all the other customers of the bank, we would call that action a personal data breach in the sense of the GDPR.

Bottleneck 2: no one is forgotten

The data structure of a blockchain means that once data have been added, they can no longer be changed. Only new blocks of data can be added to the blockchain ('append-only'). However good that may be from the perspective of system integrity, the more at odds this feature is with privacy law. According to the GDPR, personal data may not be stored longer than is necessary for the purposes for which the personal data are processed. Under certain circumstances, data subjects also have the right to have their personal data corrected, erased or the processing of their personal data restricted.

[125] On privacy issues inherent to blockchain technology, see also V.I. Laan, A. Rutjes, *Privacy-issues bij blockchain: hoe voorkom of minimaliseer je die? [Privacy issues with blockchain: how can these be prevented or minimised?]*, Computerrecht 2017/253; E.W. Verhelst, *Blockchain aan de ketting van de Algemene verordening gegevensbescherming? [Blockchain chained up by the General Data Protection Regulation]*, Privacy & Informatie 2017/1; L. Ibáñez, K. O'Hara, E. Simperl, *On Blockchains and the General Data Protection Regulation*, https://eprints.soton.ac.uk/422879/1/Blockchains_GDPR_4.pdf.

The bank must therefore amend my personal data if they are not correct, or no longer correct, and may not keep my transaction history for longer than necessary. If the bank were to record my data in a blockchain, then it does not seem possible for the bank to comply with these obligations.

Bottleneck 3: who is responsible?

In a traditional client-server model, it is usually easy to identify one or more parties who process personal data relatively autonomously. The bank provides payment services to me as consumer and to that end processes my personal data using its own IT infrastructure. The bank is the *controller* in the sense of the GDPR, in that case. The controller is the party that determines the purpose of and means for the processing of personal data and is the primary bearer of the responsibilities under the GDPR.

These matters are less clear when it comes to a blockchain. It assumes *collective data processing*, after all. A public blockchain has no owner or administrator, no central party that checks and manages the blockchain protocol. Instead, the system is maintained by a loose online community of participants.[126] This often takes place on a voluntary or semi-voluntary basis within open source projects. It does not make sense to designate a developer who is active in such a project as a controller. After all, Tim Berners-Lee is not held responsible for the processing of personal data that takes place on the World Wide Web. But who is indeed responsible for our privacy in the blockchain, then?

Case by case

Although the bottlenecks mentioned above are important and real, they do not imply that the combination of privacy and blockchain is hopeless from the start. The European Union Blockchain Observatory and Forum rightly pointed out in a recent report that it is not possible to generally point to a blockchain technology that is GDPR compliant.[127] It will always have to be looked at on a case-by-case basis whether a blockchain application satisfies the law.

This nuanced position follows largely from the fact that blockchain can be implemented in various ways. With a private blockchain, the group of participants in the blockchain can be restricted. It is generally acknowledged that this makes it easier to comply with the GDPR, for the simple fact that this ties in better with the principle of central responsibility. Another possibility is the storage of personal data 'off chain', which means the personal data are stored outside the blockchain and the blockchain itself only contains a reference to those data.

It is also an important point that the development of blockchains is still in full swing. For example, there are initiatives in the market for a private blockchain where it will indeed be possible to amend the content of the blocks.[128] The Zerocash collective is working on a privacy-friendly blockchain for a cryptocoin where the origin, destination and amount of a transaction can be screened off using 'zero-knowledge proofs'.[129]

Privacy regulator

The regulators are also orienting themselves. In September 2018, the French privacy regulator published a first analysis.[130] In that, the CNIL recognised the problem that data stored in a blockchain cannot in

[126] D. De Jonghe & V.I. Laan, *Blockchain in de realiteit [Blockchain in reality]*, Computerrecht 2017/251, p. 348.

[127] The European Union Blockchain Observatory and Forum, *Blockchain and the GDPR*, 16 October 2018.

[128] M. Arnold, *Accenture to unveil blockchain editing technique*, Financial Times, 19 September 2016.

[129] https://zerocash-project.org/

[130] CNIL, Blockchain. *Premiers éléments d'analyse de la CNIL*, September 2018, https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf

principle be amended, but it also pointed out, for instance, that data could be encrypted in a blockchain such that it could be considered 'quasi-erased' in the sense of the privacy legislation.[131]

In this same analysis, this regulator makes concrete suggestions for the allocation of roles and responsibilities in the blockchain.[132] For instance, a user that proposes a transaction to a blockchain network must be regarded as the controller. After all, this is the person deciding on the purpose of and means for the transaction. An exception would apply for a natural person who is not acting for professional or commercial purposes, since this individual could rely on the exclusion for purely personal or domestic activities.

Miners should, under certain circumstances, be considered the processor, but in any event not the controller, since their job is limited to validating transactions, without deciding on the purpose of or means for the transactions. In the event of a private blockchain, the regulator advises that a specific controller be designated, for instance in the form of a legal entity to be set up jointly. If that does not happen, there is joint responsibility and the parties must record their respective responsibilities transparently, in accordance with article 26 GDPR.

Anonymity and pseudonymity

An essential point in any discussion about privacy and blockchains is the degree to which data in the blockchain can be blocked from other users. The GDPR does not apply to anonymous data, i.e. data that cannot be traced back to an identified or identifiable natural person. In theory, a database may be entirely transparent, on the one hand, because anyone can inspect it, and on the other fully privacy-proof because none of the data can be traced to a natural person. The GDPR would not apply to such a database.

According to privacy law, however, there will not often be a case of actual anonymous data, i.e. data that cannot be traced to a person. Personal data only become anonymous once they have been (virtually) irreversibly anonymised.[133]

Every technology that does not achieve this high standard results not in anonymous data but in 'pseudonymised' data. According to the GDPR, pseudonymised personal data must be regarded as data on an identifiable natural person, to which the GDPR applies.[134] In the GDPR, pseudonymisation is included as a new definition in Article 4 (5). Pseudonymisation is defined as the processing of personal data in such a manner that the personal data can only be linked to a specific data subject by using additional information which is kept separately and securely.

Blockchain applications use various techniques to block data from other users, such as asymmetric encryption and hashing. The joint privacy watchdogs categorised these methods under the heading 'pseudonymisation techniques' in an opinion from 2014.[135] This position is hardly in dispute in the case of asymmetric encryption. After all, the private key makes it perfectly possible to decrypt the data.

There is a great deal of discussion on hashing. According to the joint privacy regulators, many hash functions are vulnerable to a brute force attack, while others believe that these techniques can indeed withstand such attacks. The debate will presumably continue for some time, if only because the technology is constantly being developed. It should be clear that it cannot be readily assumed that data have become anonymous. In a resolution on distributed database technologies recently adopted by the

[131] CNIL, p. 9.

[132] CNIL, p. 2-5.

[133] On the concept of 'personal data' and anonymisation, see Article 29-WG, *Opinion 4/2007 on the concept of personal data*, 20 June 2007; and Article 29-WG, Opinion 05/2014 on Anonymisation Techniques, 10 April 2014.

[134] Recital 26 GDPR.

[135] Article 29-WG, *Opinion 05/2014 on Anonymisation Techniques*, 10 April 2014, p. 20.

European Parliament, the Parliament itself says outright: '*data in a public ledger are pseudonymous and not anonymous*.'[136]

Conclusions

Although the privacy legislation has been formulated in a technology-neutral manner, it seems to have been implicitly set up for central databases managed by easily identifiable players. This creates a certain tension between the privacy legislation, on the one hand, and the processing of personal data within dynamic information networks, on the other. The radical network model that the blockchain introduces brings this tension to light in its full glory.

Where the GDPR can be seen as *a means for regulating centralised data managers*, the blockchain must be regarded as a technique for *fundamentally challenging* the system of centralised data management. This is a radical approach that was not immediately foreseen by the makers of the GDPR.
This does not mean, however, that the GDPR ruins the possibility of using public blockchains, as has been claimed. On the one hand, development of the blockchain technology is still in full swing and privacy-friendlier applications are being worked on in all sorts of ways. On the other hand, the GDPR has the necessary flexibility. We have seen the first signs that the regulators are willing to make the most of that flexibility. Developers of (public) blockchain applications will have to do their best. They will have to think about their applications carefully and be able to argue a solid case for why their solutions are more effective than the available alternatives, from the perspective of privacy.

Points for attention

- The decentralised and 'append-only' nature of the blockchain technology is at odds with some privacy principles, including those of keeping data processing to the minimum necessary, restricting storage and the starting point that responsibilities in relation to privacy protection must be clearly assigned.

- A private blockchain is better equipped to handle these objections than a public blockchain. Where possible, a controller must - in line with its obligations for privacy by design and privacy by default - therefore opt for a private blockchain.

- Encrypting personal data in a blockchain can be an important measure in suitably securing the personal data. As a rule, such measures will not, however, result in the data being anonymised. They remain personal data and the privacy legislation continues to apply.

[136] European Parliament resolution of 3 October 2018 on distributed ledger technologies and blockchains: building trust with disintermediation, 28.

10 Impact of blockchain on the Internet of Things

Diptish Dey and Serge Wallagh

The excitement around blockchain is inspiring a number of industries, including the manufacturing industry, to experiment with the distributed ledger technology. At the same time, the Internet of Things (IoT) and Industry 4.0 are emerging as global forces.[137] These technologies are going to have a significant combined impact. IoT relates to the connectivity of smart devices that can sense each other and communicate among themselves. IoT has significant benefits for the consumer as well as for industry, the latter often called Industrial IoT (IIoT). IIoT is expected to herald a revolutionary change and create a new working environment that dramatically impacts the way workers interact with machines. In recognition of its large-scale impact, IIoT is often referred to as Industry 4.0, the Fourth Industrial Revolution. Blockchain technology will be a part of this. As it marches forward, Industry 4.0 faces fundamental challenges that can be potentially addressed through a successful marriage with the blockchain technology.

Technology and challenges

Unlike many technologies on the Gartner Hype Cycle[138], Industry 4.0 is commercial and is being industrialised. The market size and the projections vary depending on the source. However, the consensus in 2018 is that the market in 2022 will be worth more than EUR 200 billion. Industry 4.0, or IIoT has three key drivers: efficiency across the supply chain, improved service solutions aimed at elevated performance levels and a connected ecosystem providing opportunities for new data-driven business solutions.

Key technology enablers for IoT include machine learning and advanced algorithms, hyperconnectivity, intelligent sensors and software platforms that enable human-machine and machine-machine interfaces. Machine learning[139] and advanced algorithms enable machines to improve their understanding of current and future states. Hyperconnectivity is making it possible for machines and sensors to constantly inform each other of their states. With intelligent sensors, computing power can be decentralised and brought closer to the sensors to ensure faster response times. Finally, new software platforms are facilitating the interoperability of machines and sensors of different makes and types.

The rush to innovate and grow by connecting devices in combination with emerging technologies is posing a major challenge to IoT, namely cybersecurity. In the context of Industry 4.0, the theft of intellectual property, the unwanted alteration of data and the hostile takeover of process control are serious concerns. Just even contemplating the hostile takeover of a nuclear power plant is frightening.

[137] See https://www.forbes.com/sites/bernardmarr/2018/09/02/what-is-industry-4-0-heres-a-super-easy-explanation-for-anyone/#16ff95139788 for for a detailed explanation about Industry 4.0

[138] See https://www.gartner.com/en/research/methodologies/gartner-hype-cycle voor uitleg over de hype cycle for explanations about the hype cycle

[139] See https://cqm.nl/nl/nieuws/wat-is-het-verschil-tussen-artificial-intelligence-machine-learning-en-deep-learning for explanations about machine learning and the relation with artificial intelligence (AI).

Could blockchain technology be useful in reducing cybersecurity threats and increasing the level of human confidence in Industry 4.0? Moreover, could blockchains deliver new value, new opportunities and even advance the going concern in other ways?

The role of blockchain in Industry 4.0

Although the bulk of blockchain research is related to its technology and its impact on the financial industry, the level of interest in applying blockchain to IIoT is increasing rapidly. Its potential benefit for supply chain management are currently being investigated by many companies, while some companies have already progressed to the pilot stage.

Supply chains are characterised by high numbers of external stakeholders that handle the logistics. As goods move up the supply chain, every stakeholder needs to pass on information received from his predecessor to his successor, a step that involve major trust (and therefore risk). The blockchain technology can be used to ensure consecutive authenticity and the maintenance of country of origin information throughout the supply chain.

Sustainable consumer goods: the traceability of raw materials across the value chain using digital tamper-proof documents is a major challenge in the consumer goods industry. Whether it is "From Farm to Fork" in the food industry[140] or in the clothing industry, consumers are showing increasing interest in the origin and in the manufacturing journey made by their finished products. Martine Jaarlgaard in the UK has taken a first major step in this direction. Working together with Provenance and other partners, she has launched a blockchain-based traceability project for the fashion industry. By simply scanning the QR code on an item, customers can pinpoint the origin of the fashion item. Unilever uses a similar approach to manage the supply chain of tea leaves.

Combating counterfeit products: the Gemological Institute of America (GIA) is using blockchain technology to deliver diamond grading reports as a service in a secure and digital way. This is enabling the GIA to digitally provide an independent, accurate and unbiased analysis, creating a permanent and secure record of a diamond and linking it to its current owner using his/her email address or telephone number.

Efficient supply chains: blockchain can improve the efficiency of global supply chains. These supply chains are often characterised by isolated environments with an enormous paper trail and delays caused by pending customs approvals. More than 80% of global trade volume is handled by the shipping industry as it criss-crosses multiple customs zones. Customs officials rely heavily on the correct paperwork, which specifies the product's country of origin at supplier and sub-supplier levels. Maersk and IBM are working together to explore the possibility of using a blockchain-based system to enable digital tracking and approval.

It is worth mentioning at this point that most of the blockchains used in Industry 4.0 will end up being permissioned blockchains[141]. Unlike bitcoin, a permissioned blockchain can be accessed by a privileged group of participants. This prevents unwanted access to trade secrets by unauthorised participants. How such authorisations will work in practice is currently under investigation.

Future challenges

There is hardly any doubt that blockchain technology will impact the IIoT landscape enormously in the next decades. The combined impact of blockchains and IIoT will result in substantial benefits. However, there are still a number of challenges. A business model that justifies investments in this technology

[140] See https://www.eufic.org/en/food-production/article/from-farm-to-fork for more background on this concept

[141] The website https://www.coindesk.com/ is a valuable source about crypto currencies, but also about blockchain in a broader sense.

needs to be established and the digital transformation challenge that comes with it must not be underestimated. The actual limits of blockchain technology and its possibilities and the impossibilities are still unknown. The link with IoT is still at an early stage. Aside from the technological questions, there are also many ethical and legal questions emerging. Developments in the former are expected to leapfrog those in the latter, which entails unforeseen risks.

Considerations

- Internet of Things is not a hype: it is daily reality. Application within the industry will lead to major changes. We call this Industry 4.0.

- Blockchain can be an answer to cybersecurity questions in the application of Internet of Things in the industry, or beyond.

- Blockchain already delivers direct value within Industry 4.0 by increasing the efficiency of global supply chains.

- Insufficient consideration has been given to the legal and ethical consequences of IoT within the industry in combination with blockchain.

11 From client to vendor relationship management

Leon van Ekeren

Today's consumers often behave in a schizophrenic way. In the physical world they expect to be treated as kings while in the digital world they settle for the role of 'dummies', allowing themselves to be exploited through commercial surveillance. In both environments, a variety of consumer relationship management systems (CRM) store their activities unnoticed and usually unsolicited. That data is constantly and automatically enriched in order to approach people with the sharpest possible focus. Because although we tend not to accept manipulation and violation of our privacy as consumers, everything changes with the introduction of vendor relationship management (VRM). With this new approach, the buyers of products and services are in control rather than the vendors. The buyers determine from whom they obtain information and with whom they exchange data or perform a transaction. In other words, they manage their own personal data themselves and ultimately dictate the terms of delivery. So VRM in combination with blockchain-based applications will fundamentally change our economic reality.

Research project

The 'Project VRM'[142] at Harvard University has been working on the development and promotion of *vendor relationship management* (VRM for short) since 2006. Worldwide, people and organisations are being encouraged to think along and build tools that make the concept possible. They are getting better and better at it and various platforms are currently being tested on a smaller and larger scale. Examples in the Netherlands include the IRMA project and TrustChain / Digital Stamp, while Solid-Inrupt is a globally appealing project. All three are the *actual personal digital data vaults*: the VRM base from which VRM applications communicate. For a long time, technology was the bottleneck for implementing VRM, but that hurdle now seems to have been overcome. A new commercial reality is emerging in which the physical consumer corresponds much better with his digital alias. Blockchain technology can help to make storing (possessing) and transporting data superfluous. With VRM, just organising access to data is enough to get an answer to a question and therefore be able to carry out a process or action requested by the consumer.

[142] Project by the Berkman Klein Center for Internet & Society, Harvard University

Example

Suppose Mrs. Jones wants to buy clothes and enters a random boutique. The saleswoman who approaches her seems to know her. Without having exchanged a word with her, she is suspiciously good at estimating what Mrs. Jones is looking for. She knows her size and style preferences and also shows that she has a good idea of Mrs. Jones's budget. To Mrs. Jones's question of how she actually knows all these things, the salesperson confesses: 'We buy this information from an organisation that's following you everywhere'. There is a good chance that Mrs. Jones will exit the boutique without spending a cent. But what so obviously cannot exist in the physical world is the most common thing in the digital world. So it is foreseeable that the digital world will adapt to the customs of the physical world. The ideas have been around for a long time and now the technology is ready for it. Customer can start working on the recovery of their position of always being right**.**

Ads and more

Although the internet has acquired an important place in our lives over the past 25 years, it is still a world in itself. A separate space, where most people are still 'naked' in a way. Because, unlike the physical world, there are as yet no socially anchored standards about what is private and how to deal with it[143]. Because the implications of issues such as 'Who owns personal data' were overlooked at the start of the digital era, everyone simply assumed we could store and process everyone's data.

As a result, the web now has a built-in commercial surveillance system that collects as much personal data as possible, unsolicited and unnoticed. Most of the time, it is used to create tailor-made advertisements, which are presented unannounced and as smartly as possible. It is a multibillion business in which, besides the big five (Amazon, Apple, Facebook, Google and Microsoft), hundreds of unknown data-tracking companies are making unprecedented and enormous profits. Literally at the expense of the internet user, who is actually powerless. But there is hope for the consumer because there are techniques such as blockchain under development, which can more effectively protect the data sovereignty and privacy of consumers, citizens and employees..

Organising things differently

Such a skewed business model is screaming for an alternative, which is why many parties are working hard in this area. The overall concept is called Vendor Relationship Management and is seen as a counterpart to customer relationship management. The purpose of CRM is to promote third parties from suspect to customer as quickly and as cheaply as possible. Ultimately, organisations with CRM want to attract other customers and business relations.

Today's internet is fully equipped for this. VRM turns it around and puts customers in the 'lead' by giving them full control over their own personal data. They determine which party is allowed to use which information. This approach is not just much fairer for consumers, it is also ultimately more advantageous for advertisers because they can expect better quality information from customers and prospects in a cheaper and fairer way. Organisations no longer need to own data. Using blockchain technology, an organisation's server can pose questions to digital data portals managed by consumers themselves. With the answer, only those actions can be performed for which permission has been given.

[143] Doc Searls; https://medium.com/@dsearls/for-privacy-we-need-tech-more-than-policy-b681e527daab

Portal

The starting point for VRM is that individual customers have their own portals for searching for and booking products and services and carrying out transactions. Because VRM focuses on customer-driven leads, the portal must also provide customers with the tools needed to deliberately commit to the provider. Customers decide for themselves whether they want to do business with a particular supplier and, if so, which agreements the supplier must comply with. This process has many similarities with building and maintaining a customer-supplier relationship in the physical world before the advent of the commercial internet.

The aforementioned portals are secure Identity Platforms, or digital data vaults, with which individuals and organisations can manage all their (confidential) data themselves. In practice, such a data vault has the form of a web page on which the customer specifically indicates who is allowed to access which data, for which purpose and when. Identity Portals are not necessarily based on blockchain technology, but they are perfect for use in blockchain applications.

Worldwide

The development of these digital portals is being worked on all over the world – and in the Netherlands too. Examples include the IRMA project at the University of Nijmegen[144] and TrustChain / Digital Stamp at Delft University of Technology[145]. Both projects include platforms that allow users to authenticate themselves using an app based on one or more attributes in combination with their various roles. By using a 1-to-1 relationship between the user and service provider, the user can purchase or accept services anonymously without a password and with a minimum of required attributes. The difference is that TrustChain, unlike IRMA, is based on the principle of blockchain. Applications on both systems are now being tested in a number of Dutch municipalities. The advantage of a platform based on the distributed ledger (blockchain) principle is that smart contracts and cryptocurrencies can ultimately be used as well.

Open source software

The Solid[146] platform, devised by World Wide Web creator Tim Berners-Lee, is currently in the international spotlight. With Solid, individuals and organisations also manage their own data vault, called Solid-POD (Personal Online Data). Solid is a completely open source and Berners-Lee is explicitly inviting everyone to develop applications for it and to adapt existing ones.

The various parties must work simultaneously to successfully implement decentralised data platforms. The platform provides the infrastructure, while customers must manage their personal data on the platform and providers must make their applications (and also their CRMs) suitable for communicating with the platform protocol. In itself, this is not difficult and as VRM systems become more established, implementation will accelerate mainly in the business-to-consumer market. However, that doesn't mean that CRM systems will disappear. Over time, their function will change into databases that communicate relatively autonomously with the VRM tools used by customers – in other words, communication and data exchange based on equality.

[144] https://privacybydesign.foundation/irma/

[145] https://www.tudelft.nl/2018/tu-delft/tu-delft-bouwt-mee-aan-een-digitale-identiteit-voor-op-de-telefoon/

[146] https://solid.inrupt.com/how-it-works

Attractive benefits

It is expected that internet users will soon choose to do business through their personal VRM portal, where they no longer need to remember user names and passwords. Verification is automatic and is also much safer. The power of the big five and smaller data trackers will eventually decrease and these companies will earn less. That money can then be invested in much better and more appropriate offers to the customer. This also will mean that the relationship between providers and customers in the digital world look more like their relationship in the physical world.

Conclusion

Vendor relationship management ensures that customers can do online business with suppliers (providers) on the basis of equality. Providers are all organisations with whom the individual has an online relationship, such as businesses, governments, schools, etc. VRM will make all types of customers more productive because they will only need to manage their data in one place and log onto 'linked' providers.

However, providers will have to invest to make their CRM systems suitable for communicating with the VRM tools of their customers. For individual providers, that investment will result in a direct digital relationship with their customers. At the same time, they will no longer be obliged to protect customer data . Many VRM tools will work with blockchain principles so that providers and customers can work with smart contracts and digital payments. The acceptance of VRM will also stimulate the development of blockchain.

Points of focus

- In a nutshell, VRM is for customers what CRM is for providers: a database from which they manage their online relationships with their suppliers.

- Essential for VRM: secure identity platforms or 'data vaults' that enable customers to manage, control and distribute their personal data. Based on these platforms, providers build applications to communicate with customers and exchange information on conditions accepted by both parties. Blockchain technology seems to be very suitable for this.

- With VRM, providers no longer need to store customer data in their CRMs, but just need permission to request such data for each attribute. That will significantly reduce the risk of the accidental leakage of personal data.

- With VRM, customers regain their autonomy and their natural role in their relationship with suppliers – in both the digital and the physical world, because the two worlds will increasingly coincide.

12 EDP Auditing and blockchain: blind faith or auditable trust?

Robbert Johan and Maarten Souw

Is an IT system and the information it contains a reliable and useful representation of the truth? This question describes the essence of the digital auditing profession. The nature of the engagement can involve anything from assessing network security and specialist assurance to verifying the EDP-dependent parts of a financial statement. The IT auditor tests whether the information provision and underlying technology provide a reliable and complete picture of the actual transactions and rights. In this article, we argue that the competences of an auditor could similarly be used to verify the correct implementation of smart contracts in blockchain. Given the unsupervised functioning of smart contracts, the completeness, accuracy and irrefutability of the transactions are crucial.

It's all about the application

The impact of blockchain technology on organisations is a question that is frequently asked by CIOs, senior IT management or even line management. Blockchain appeals to many people and the discussion has its distinct protagonists and doubters. Instead of repeating these discussions, in this chapter we want to explore the implications of blockchain for the field of auditing.

Blockchain is an innovative application that is used to set up a confidence model without the need for a central authority. It is precisely the absence of a trusted third party that is interesting, and for two reasons. Blockchain – because it obviates the need for a central authority – enables challengers to attack existing market models and monopolies. The disruptive potential of blockchain has attracted the attention of senior management and should therefore concern the audit professional.

The second reason is more technical and follows on from the distributed design. With the absence of a central authority, the trust of the user community (reliance) depends mainly on the quality of the implementation. The reasoning is that the design philosophy of blockchain – a self-controlling network of intelligent nodes – is tried and tested, but that the application of the blockchain could be erroneous. We therefore suggest that an IT auditor should assess whether the application of blockchain meets a company's expectations.

Case study registry and opposing interests in Ethereum

For this article, we take an Ethereum-based solution as an example. It should be borne in mind that the original example is based on the Dutch system. According to Dutch law, certain registered goods such as houses or yachts can only be transferred through a notary. Building an alternative solution in blockchain would be interesting – either to fulfil this function where no register exists or even to provide an alternative to the existing registry.

To fully understand this application of blockchain, we need to examine the two ways in which Ethereum is used:

- Ethereum has one application as a crypto, which implies that the correct functioning of the Ethereum infrastructure has been critically tested many times.

- Ethereum can also be used as a platform for smart contracting. Here, a party realises a customised solution based on Ethereum. It is precisely for this type of new application that a test by an IT auditor adds value.

This statement needs to be explained. Ethereum consists of a network of Ethereum virtual machines (EVM). These EVMs are housed on various host machines and they process smart contracts and record the executed transactions in a blockchain. The standard smart contracts processed by EVM are payments in Ethereum. Ethereum expressly allows the use of its own set of smart contracts in addition to the Ethereum coin. The technology has a scripting language that developers can use to design their own smart contracts and process the EVMs.

Opposing interests

We can take the standard application – as a means of payment – as a tried and tested solution. The (Ethereum) blockchain represents a certain value, because users record their claims and obligations as a transaction in this system. These participants have opposing interests: the obligations of the delivering party are the rights of the receiving party and vice versa. This conflict of interest also means that all parties have a vested interest in confirming that transactions in Ethereum are trustworthy and correct. We can therefore safely assume that any errors in Ethereum will soon be detected and rectified. This confirms the correct functioning of the standard Ethereum coin and infrastructure combination.

As mentioned above, the Ethereum infrastructure allows for new uses such as the sale of a yacht by means of a smart contract. By tracking the payment for and transfer of the yacht in an Ethereum blockchain, we could obviate the need for a register. For the sake of simplicity, let us validate a simple transaction. Peter wants to buy Paul's yacht for EUR 50,000. So if the yacht is registered to Paul and Peter transfers the money, Peter becomes the owner of the registered property. Translated into algorithms, this process involves three steps:

1. If the yacht is in Paul's name in the Registry, then
2. EUR 50,000 will be transferred from Peter's account to Paul's account, and then
3. The yacht will be registered in Peter's name.

The *if-then* algorithm is the basis for the smart contract. The transaction is recorded in a blockchain – which cannot be mutated due the infrastructure of the blockchain – making it an alternative authentic registry.

Auditing blockchains

Trust, or rather reliance on our prospective registry in blockchain, needs to have a basis. This basis can be in the shape of a tractable assessment of the reliability of our blockchain solution. An IT auditor can typically assess the inherent risk and certify the security measures.

The IT auditor will first determine the right risks during the preparatory work and the performance of a risk assessment. Based on their impact, the appropriate control approach will be determined. For our essay, we focus on the risks involved in building a new application in Ethereum. Any new subroutines built on the Ethereum infrastructure are generally not tried and tested. For the time being, the infrastructure can be assumed to be a trusted computer base.

Returning to our new application – the prospective registry – we can identify risks regarding A) the use of the blockchain, B) the translation of the smart contract to the scripting language and C) the context of the blockchain solution.

Suitability of blockchain

For question A – Is blockchain the appropriate solution? – there are two typical risks.

1. How resistant is the encryption technology to attackers? Given the importance of the underlying business deal, our registry needs to be tamper-proof or at least tamper-evident. Blockchain uses cryptographic security features (hashing) to ensure the authenticity of transactions. It is important here that the chosen encryption is also safe in the longer term. Most IT applications usually last longer than expected, while the capabilities of hackers increase every year. The risk of the encryption becoming quickly outdated must be weighed up.

2. In which way are transactions validated and is this done using a public-private key infrastructure? Is it a public or a private blockchain and where is the 'power' to mutate the blockchain (especially technically)? The presence or absence of a central authority has an impact on the risks to be investigated. For example, a central authority has the advantage of blocking malicious parties from the blockchain. On the other hand, the availability of the blockchain application depends on a single point of failure. A public (open) blockchain has exactly the opposite benefits and disadvantages. The blockchain no longer has a single point of failure, but there is no central authority to bar undesirable actors.

Inherent business risks

Risks in the translation of the business model to scripts (B) exist on a legal, business-economic and functional level.

1. In which way is the privacy of the users guaranteed? The processing of personal data is sometimes underestimated when blockchain technology is used. The cryptographic techniques must guarantee irrefutability. It may well be that the security of personal data has yet to be realised separately.

2. Not all organisational issues can be solved quickly by blockchain. For the legal transfer of real estate in the Netherlands, for example, it is well organised. Transporting smaller registered goods or moving registered goods across the border is much more challenging. The resolution of this type of problem is a skill that is also being demanded more by IT auditors, even though the shift in expectations towards the IT auditor is separate from the blockchain developments.

3. The functional risk is fairly predictable. Are the scripts a good translation of the intended business processes? This concerns an almost classical system audit in which the IT auditor validates the translation of the business process to the system. Particularly the development and testing processes are not considered for testing.

Operational and technical risks

In the context of the blockchain solution (C), we see risks in the areas of infrastructure, identity management and operations management.

1. The application used to build the registry will in all likelihood contain a plethora of subcomponents. Items such as application programming interfaces, user interfaces, program logic and the central database spring to mind. For all of these parts, the auditor needs to make sure that

they are properly set up. In addition, the components need to work well together. To return to our example, the way the registry has used the APIs should be examined. Has the developer correctly applied the specifications of an API? Because this determines the proper functioning of the blockchain. Where and how the databases are housed influences the confidentiality and availability of the solution. Blockchain may safeguard the integrity of the transaction, availability and confidentiality and still be dependent on the lower IT levels such as servers and networks. The user Interaction and user interface are also an interesting sub-domain. An application that does not adequately meet OWASP (or similar) requirements does not provide sufficient protection against malicious attackers. Here, too, a solution that was adequately secured last year can quickly become outdated.

2. In what way is the identity of an individual guaranteed? Because the transaction is processed without human intervention, the risk of identity fraud must be assessed. The IT auditor should therefore assess the management of access resources, such as tokens and user management processes.

3. How is the application managed? The need to adapt the application as a result of changing user requirements is obvious. This means that the application must be supported by a type of change management. As we already know, blockchain has the special feature that historical transactions are in principle immutable. A change in the contract may require a fork. The IT auditor should ask how such a decision will influence the management processes.

Conclusion

For an IT auditor, blockchain technology has an impact on the required IT technical expertise. We expect that the process of investigating blockchain will deviate little from the existing audit topics. The IT auditor will examine the commitment, the functional needs of the company and the management of blockchains. Particularly in the first area, more will be asked of the IT auditor, but this is a trend that has been prevalent for some time. The profession should therefore develop a mid-term vision.

On the other side of the spectrum, we expect that the IT auditor will usually have the knowledge required to assess the current management and design processes. This will lead to the main shift in the requisite technical knowledge. For example, IT auditors need to understand the operation of and the technology behind and around blockchain. They must be able to assess whether a blockchain with a simpler hashing algorithm offers sufficient guarantees in the longer term. An up-to-date picture of cyber threats and security technology – in addition to a knowledge of the most important blockchain technologies – is an advantage.

Suggestions to the profession

To summarise, the main message to the IT audit community is that:

- We need to develop an understanding of the foreseeable consequences of blockchain development.

- We must deepen our understanding of the main blockchain versions.

- We should be able to map blockchain developments properly in the domain of cybersecurity.

13 Identity and authentication organised differently

Vincent Hoek

People 'build' organisations because they're convinced they can achieve more with them than without them. Their reputation and legal validity require a degree of trust and confidence that has become greatly dependent on measurability, thanks to digitisation. Processes handled by people (People-Based Processing - PBP) are being replaced by processes handled by machines (straight-through processing -STP). Digitally-supported process handling ideally takes place on the basis of verifiable and trusted identification and authentication of all people, machines, organisations, processes, applications and datasets involved.[147] Where trust is based on personal contact and official documents in the traditional world, in the digital society trust must be earned by comparing attestations. Blockchain technology has made this possible. On the one hand, the intermediary no longer plays a role in control and risk management, while on the other hand a compelling amount of regulation requires certainties that will have to be substantiated with justifiable trust.[148]

Social drivers

Society is developing from data *management within* organisations to *data exchange between* organisations. For example, agencies such as www.gleif.org and www.gs1.org provide a complete range of data trust anchors. Data relationships affect every supply chain: manufacturers, distributors and operators are all responsible for their visibility, efficiency and safety. Standards simplify the underlying processes that enable users to speak a common language to share trusted information. However, standardisation and governance models are not yet fully developed.

This is resulting in increasing complexity due to rapid change and globalisation, which is presenting opportunities for fraudsters that are hiding behind the anonymity of the internet. Does an organisation really exist? Are information claims correct? Digital-based trust requires (i) an increasingly sophisticated contextual notion of the authentication of an identity, (ii) orchestration of the ecosystem to clarify the

[147] According to the World Economic Forum, these five technologies could potentially change world trade https://www.weforum.org/agenda/2018/06/from-blockchain-to-mobile-payments-these-technologies-will-disrupt-global-trade/

[2] Especially the European legislators are trying to regulate the data explosion:

• The eIDAS regulation is about citizen eID Authentication and digital signatures, which help each EU state to trust each other's citizens crosswise (federally).

• The Dutch Network Information Security Directive (NISD) sets standardised requirements for the design of digital security.

• The General Data Protection Regulation requires purpose limitation for the processing of personal data and ensures that pseudonymity is set up to the level that a person is no longer identifiable.

• The 4th Anti Money Laundering Directive (AML4) regulation provides guidelines for customer due diligence checks, the reporting of suspicious transactions, the keeping of payment overviews, money laundering and the financing of terrorism.

• The Payment Services Directive (PSD2) requires registers to be kept of persons with a substantial interest in financial transactions. For example, the world money market is becoming more transparent, but attention is also being paid to digital payment transactions in a way that contributes to the flexibility of cross-border payment services and new forms of financial services such as (cyber) insurance.

context and (iii) access control in a pallet of increasingly automated, logical interactions between people, machines and corroborating organisations.

Benefits

We can achieve trustworthy Straight Through Processing with an identity ecosystem framework that uses *online, cross-trusted claims* that underpin their legal legitimacy. These claims can be retrieved and compared in a federated and distributed network of trusting registers, called a Register of Legal Organisations (ROLO).

With increasingly interwoven delivery channels, a growing demand by end users for ease of use, service quality and effective management of the corporate identity, the advantages are clear:

- the reduction of the administrative burden and coordination costs;
- improved and renewed services at lower transaction costs;
- the reduction of (fraud) risks, increasing the general trust and improving organisational security.

Also end users are improving their position with better identity assurance:

- customers can put more trust in a company's reputation;
- the desired service can be purchased more efficiently.

Register of Legal Organisations

The realisation of these wishes is mainly a matter of the degree of coherence between identification, trust and the required degree of certainty that assumptions and expectations are justified (assurance). Standardisation institutes call this concept Level(s) of Trust and Levels of Assurance (LoA).

The Register of Legal Organisations (ROLO)[149] has been developed in the United Kingdom because today no company can grant a decent Level of Assurance to an employee if it is not at the same LoA level (or higher) and is recognised as such. ROLOs are cross-trusting mutual references to distributed and federated registers of the attributes that help to clarify the legitimacy of an organisation, its assets and staffing, based on comparing data such as names (including the Ultimate Beneficial Owner), licence plates, bank account numbers, (location) address(es), Chamber of Commerce number(s), land registry number(s), granted licence(s), transaction history ... the list is infinite. The first ROLOs are now gradually becoming operational.

The more digital technology is rolled out, the easier identification should be. The rule should be that the bigger the digital footprint of an organisation, the more opportunity of fraud and digital security incidents.

In the end, everything revolves around verifiability. The challenge when carrying out the necessary verifications is to check the presented claims against authoritative sources – that is, data sources collected under a recognised mandate at a verifiable data quality level (such as ISO 8000), the results of which are stored in a blockchain, for example.

Organisations will face mounting pressure to prove the authority of their data because:

- organisations are constantly changing
- the work population is also constantly changing
- key management based on asymmetric encryption has become more complex on mobile phones because operating systems, data containers and cloud apps are becoming more loosely connected.

[149] Distributed Ledger Technologies for Public Good: leadership, collaboration and innovation, [pg 13] http://chrisholmes.co.uk/wp-content/uploads/2017/11/Distributed-Ledger-Technologies-for-Public-Good_leadership-collaboration-and-innovation.pdf

Organising interoperability

Traditionally, *files* are linked between *applications* to enable digital collaboration. This is done directly by programming links and indirectly by querying the data through a hub. Today, we can more easily query '*pieces of data (attributes*)' on the basis of claims within a framework of strict conditions (policies). Data owners define requirements that must be satisfied by data requesters.

This makes the error-free processing of data sets possible without having to link complete applications. For example, we can ask for 'number' and not for a 'type', or we can ask for a 'shipper' and not for a 'paying party'. Actors only request data aspects that they need to carry out an identifiable action, and for this purpose the linking of the data under GDPR is guaranteed. Using a cross-referenced checklist, we could verify the similarity of available data attributes in federated registers of various stakeholders to check whether an organisation is legitimate. Its legitimacy is evident from all the referenced data that should be available to authoritative data sources if and when the organisation operates legitimately, augmented by a range of open data sources.

Example

If someone claims to have a private company, the law states he must pay taxes for which a VAT number is required. In the Netherlands, this is only available through the tax authorities, after which the party is registered by the Chamber of Commerce in the Dutch Commercial Register (NHR), with its Ultimate Beneficial Owner listed in the UBO register. Correlation of this data with bank account numbers and real estate registers, but also with rented means of production and permits such as machines and vehicles and with legal documents such as inventory permits, makes fraud more and more difficult.

The required blockchain environments are rapidly becoming more user-friendly, including management challenges such as recovery, rotation and secure access.

What is needed now is a new verification method of identity and authenticity.

Three dimensions of identity assessment

1. For citizens, the government is responsible for the individual's identity (basic registration, passport, etc.). All other means of identity, such as a driving licence, are derived top down. This model is under pressure, because more people are coming online whose national governments are unable to provide a reliable identity. *The traditional government model of identity assessment no longer works.*

2. Modern states use a so-called early-bind model, i.e. check first and then provide a token. With the so-called *Self-Sovereign method*, the user receives a blank signed token without a trust-based connection. That rust can be earned by making claims that are added to the token after verification. In this way, a growing wallet of attestations is created, from parties that indeed subscribe to a claim that is made. However, the underlying process is invisible, so the trading partner does not actually know how the data came about. This model places the power over determining identity in the hands of Internet companies, which claim to be able to facilitate reliable self-sovereignty. *Internet companies do not formally have a mandate to issue identities, but they are technically better off than governments.*

3. The third approach is Zero-Knowledge Proof (ZKP). Finding out whether the data that an actor has in common with the data held by a government organisation or other authorised source, requires

mathematics. Without a match, the data is not correct and additional data needs to be found. Thanks to ZKP protocols, all relying parties can keep each other up-to-date if data is invalid. A legitimate party that has nothing to hide can give permission for this and this type of agreement ensures that the relevant data is always correct. *The combination of Self-Sovereignty with ZKP makes federated ROLOs possible*.

Decentralised identities

A combination of these three identification methods creates a decentralised identity incubation that can function as the backbone of modern business operations. Partly under pressure from data breach and identity theft, users need a way of becoming owners of their identity. After research, blockchain technology and protocols are now suitable for facilitating decentralised identities (DIDs). In addition, we can now technically combine the aforementioned three dimensions of identity identification.

DiD is characterised by privacy by design. By using secure encrypted digital hubs – which can communicate with users' data while respecting their privacy – the veracity of the identity information of people, machines, organisations, applications and individual data sets can be verified in an ecosystem of suppliers and purchasers.

Conclusion

Trust must be earned by everyone but is provided by a community. Where traditional identity systems focus on authentication and access control of imposed tokens, new concepts (DiD, ZKP and ROLO) add the *contextual verification of the authenticity* that a community can (re)establish in the confidence of claims by cross-referencing data sources. In a decentralised system, trust is based on certificates: claims endorsed by other entities. This approach helps to prove aspects of identity. With federated distributed ROLOs, the certificates can be compared real-time between disparate authoritative sources and relying partners, enabling specific levels of identity, trust and assurance.

Considerations

- The creation of a new robust and resilient, decentralised and also federated identity ecosystem that is accessible to everyone worldwide requires standard open source technologies, protocols and reference implementations. Blockchain technology and protocols seem to be extremely suitable for facilitating decentralised identities (DIDs). In addition, government organisations will have to perform a robust reality check, because the traditional early bind model with central identity platforms is not up to the challenges of the network society.

- Relying partners are parties that have as much to lose as their own organisation if the requested information is not correct. For example, a bank wants to know for sure that a mortgage will be repaid on an asset that is known to the Land Registry, whose address can be registered as a business at the Chamber of Commerce. DIDs, ROLOs and ID hubs based on blockchain technology assist their members in an ecosystem to access an increasingly accurate set of certificates, while helping to reduce regulatory compliance risks by only processing these data attributes instead of checking identities and files on behalf of the user.

14 Programming blockchain software in open source

Victor de Pous

In the past, open source software emerged as a silver bullet against vendor lock-in situations thanks to the free availability of the source code. The now widely accepted deviant contract model evolved entirely differently. Open source is mainly used when reusing software components to allow a short time to market. The royalty ban can also function as a driver for acquiring market share, as Android has shown, worldwide even. The open source model plays an important role in the development of a blockchain. All sorts of parties can program jointly in a decentralised manner, while users pay no licence fee. All of this opens the door to rapid rise and broad acceptance. Like other legal issues in relation to blockchain applications, the legal aspects of open source software probably do not receive enough attention. Which is unfortunate, because the type of open source licence is important for the objective of the project and can also influence the adoption curve.

Back to basics

Fifteen years ago, proponents and opponents to open source software found themselves directly opposite each other, in an emotional debate. Today, the ranks have largely closed. Open source software pertains to a globally-accepted legal phenomenon that theoretically started in the 1980s as 'free software'. A social movement against the established ICT companies who curtail users' freedom and cause undesirable supplier-dependency with their proprietary runcode-only software.[150]

Even the most notorious criticaster of yore, the Microsoft Corporation, slowly but surely changed course after the departure of CEO Steve Ballmer in 2014. On 4 June 2018, the company even announced it was taking over the GitHub open source platform.[151] Four months later, Microsoft joined the Open Innovation Network and made its portfolio of 60,000 software patents available for use free of charge to this 2,600-member Linux community, including indemnification against intellectual property claims.[152]

Everyone may have an opinion on it, but open source software is, fundamentally, a *legal construction for* the development and public, free availability of software source code, whether this takes place as part of a collective effort or otherwise, in a decentralised manner or otherwise. From large operating systems, like Linux and Android, to all sorts of components; including libraries and application programming interfaces. Specifically, it is only the licence agreement that makes the code 'open source'. Open source software, including the stricter model of free software, is a varied collection of software licences that are *divergent in character*. It goes without saying that every developer, supplier and user must comply with these special licence terms and conditions in the concrete case, but preferably must

[150] For an overview of developments in this domain, see: V.A. de Pous, *Open source software en politiek [Open source software and politics]*, Amsterdam, 2004. From the same author, *Open source software*, in the compilation *Digitaal recht voor IT-professionals [Digital law for IT professionals]*, Amsterdam, 2016.

[151] For 7.5 billion dollars (https://news.microsoft.com/2018/06/04/microsoft-to-acquire-github-for-7-5-billion/). The European Commission gave approval for the acquisition on 19 October 2018.

[152] https://azure.microsoft.com/en-us/blog/microsoft-joins-open-invention-network-to-help-protect-linux-and-open-source/

first take into account what the special ground rules entail and what implications this has for the operations.

Deviant contracts

Like computer programs that are provided on the basis of traditional licences, open source software is not work that is in the public domain to which the maker has waived his intellectual property rights. In other words, open source software is - always - subject to copyright and possibly patented. Saying that such software is 'royalty-free' or 'licence-free' is wrong, therefore.

In principle, all open source licences share the following special characteristics. The licensee acquires the right to run the runcode an unlimited number of times and for any purpose and also the right to copy, edit (examine and amend) and further disseminate the source code of the software; both the original and the amended version. No fee may be charged for use.[153] With these attractive advantages or freedoms, there are no contractual guarantees or certainties. Take, for instance, the authority to provide the software, indemnification of users against intellectual property claims from third parties and guarantees that the software has a certain functionality or is operable and works according to written specifications. Furthermore, the liability of every maker (programmer), for instance for errors in the software code, is excluded.

That last point has traditionally been a weighty point of dispute; also in the light of peer-to-peer review of each other's programming work, which emerges in practice to work - sometimes and perhaps increasingly - insufficiently. With all the consequences that entails.[154] This matter is given a new dimension by the Dutch government's policy intention to encourage companies to make software safer via a special form of software liability[155]. The maker, distributor or supplier of software for a blockchain does not escape this. Certain clauses in open source licences could be null and void or nullifiable by operation of law in future on this ground, which would mean individual programmers could nonetheless be held liable.[156]

Unavoidable licensing problems

The ease with which the unique basic rights can be identified belies how complex open source proves to be legally in practice. This is due to two parallel circumstances. On the one hand, countless open source-type licences have been written - some count no fewer than 2,500. On the other hand, the individual user terms and conditions create confusion. So it is unclear what exactly should be understood under 'derivative work' and 'distribution', or which (national) law applies between contract parties.

Another question concerns the remarkable self-regulating character. The Free Software Foundation (FSF) judges the qualification of 'free software' based on its own 'four essential freedoms' with which the licence agreement must comply.[157] The Open Source Initiative (OSI), on the other hand, likewise a US foundation, *certifies* the licence agreements based on 'ten criteria'.[158] 83 licences have since been 'OSI-

[153] This last right, for instance, prompted the city of Barcelona to switch partially to open source software at the end of December 2017. The change is supposed to save 70% on licensing costs. A number of Microsoft products are in any event being replaced. https://elpais.com/ccaa/2017/12/01/catalunya/1512145439_132556.html

[154] According to reports, a crucial security error, later dubbed Heartbleed, in OpenSSL made *two-thirds* of the immense World Wide Web vulnerable in 2014 (https://en.wikipedia.org/wiki/Heartbleed).

[155] Coalition Agreement 2017-2021, *Vertrouwen in de toekomst [Confidence in the future]*, of 10 October 2017.

[156] All things considered, that is also the case now. Based on general Dutch contract law, after all, no single contract party can exclude its liability for gross negligence or intent.

[157] http://www.gnu.org/philosophy/free-sw.html

[158] https://opensource.org/osd

approved'.[159] Besides the observation that the lion's share of open source projects probably make use of approximately ten different licences, a supplementary, but indeed approximate, way of creating order in the chaos could be found in distinguishing between user terms and conditions with (i) a *restrictive* - 'copyleft' - and (ii) a *permissive* character.

Viral effect

A restrictive licence prohibits the licensee from, *in the case of distribution*, removing the software from the sphere of free availability once it has been amended (*derivative work*). The licensee may not, therefore, offer the software as *proprietary* software in exchange for payment of a usage fee. And: when the software is disseminated, the same open source licence as applies to the original software must apply in full. Furthermore, in the event of copyleft licences, there may be a 'viral effect'. If, in the event of 'composite software', a piece of code with the copyleft terms and conditions is *directly* included[160], this component legally 'contaminates' the code base. With the result that the particular copyleft licence immediately and usually unintentionally and undesirably applies for the entire computer program.

A permissive open source licence, on the other hand, gives the licensee the right to, in the event of distribution, pull the changed software from the sphere of public availability via a traditional licence. The party doing this must, however, in this case mention both the (i) copyright and licence notice and (ii) the disclaimer of the permissive licence if the open source portion is substantial. The most widely used permissive licence agreement is the MIT License, which makes, among other things, the Bitcoin core[161] available, while the popular platform Hyperledger Fabric[162] is offered under Apache 2.0; likewise permissive in character.

A blockchain project can become legally complex in terms of software licences. Looking to the near future of Ethereum: the core will be available in future on the basis of a permissive licence, while for applications, the Ethereum Foundation has in mind the General Public License version 3 (GPLv3) and for middleware, the Lesser General Public License version 3 (LGPLv3).[163] These last two licences are based on the copyleft principle, but only the first one mentioned has a strong viral effect.

Blockchain

Not everyone realises that blockchain technology is booming more or less thanks to the open source model. Open source software is about software (in source code). Blockchain software generally consists of three segments, specifically cryptography (security), distributed ledger technology (DLT) and a decentralised system. Any computer program (or even a component thereof) *can* be open source.

A remarkably high number of these open source projects do not take root, but the code does in principle remain publicly available. For instance, 26,000 blockchain software projects were started on the GitHub development platform in 2016, but only 8% of these were still active in November 2017.[164] This does not change the fact that every one of these projects has its legal basis in open source software and is further provided for in one or more specific licences. A mix of restrictive and permissive user terms and conditions (hybrid) is often involved.

---

[159] Please note. An approved licence says nothing about the legal quality and legal validity of a licence generally nor anything about the functionality and quality of the software code itself.

[160] In the event an open source licence has a viral effect, the method used to 'link' the software components, such as *integration*, *aggregation* and *(static or dynamic) linking,* plays a role. This aspect prompts disagreement.

[161] https://en.wikipedia.org/wiki/Bitcoin_Core

[162] https://github.com/hyperledger/fabric

[163] https://github.com/ethereum/wiki/wiki/Licensing#the-core

[164] https://www.cnbc.com/2017/11/09/just-8-percent-of-open-source-blockchain-projects-are-still-active.html

Conclusions

Precisely if programming blockchain software (the development side) also involves combining existing open source components, very targeted attention to licence compliance (compliance with *all* the terms and conditions of the particular open source licences) is required. Developer, distributor, supplier and user must always adhere to these specific licence terms and conditions (even if use is 'free of charge') and they would do good to also take into account the special legal nature of open source software.

Of even bigger, in fact primary importance is, however, the *choice of licence* for the blockchain software (the production side), which should depend on the objective of the initiator(s). This decision can influence the adoption curve. A permissive licence offers the possibility of commercialising the software as non-open source, if desired; a stricter copyleft licence does not allow that.

Analyses

- Open source software is a collection of *deviating* legal constructions for creating and disseminating software code - with many freedoms but no guarantees or certainties for the user, and *always* within a framework of contractual terms and conditions, based on copyright law (and sometimes also patent law). Open source software offers excellent opportunities for developing blockchain software because in principle, anyone can 'program along' (locally), (discrimination is even contractually prohibited) and the blockchain can rapidly scale up on account of the absence of any licence fee.[165]

- For a blockchain, too, the advantages of open source software are only achieved in practice if a party or organisation acts carefully, so in accordance with every licence and with supplementary legal guarantees and certainties; also for quality and continuity.

- On top of this, the choice for a (i) restrictive (copyleft) licence or (ii) permissive licence is based first of all on the *envisioned (economic) goal*, while this decision can also have an impact on the *adoption curve* for a blockchain project.

- Where (i) licence non-compliance traditionally posed the most serious legal risk, other kinds of risks have now explicitly emerged. Quality issues. On the one hand, this concerns (ii) 'open source insecurity': security defects which could allow value to be stolen, a system outage or a privacy breach, for instance. On the other hand, (iii) general functional code quality risks have started to weigh more heavily in open source software.

- Because of its choice for a detailed legal mix of open (Android core) and closed software products (Google Apps), Google has managed to secure an 80% monopoly on the immense global market for mobile OS in ten years' time. At the same time, Google has successfully managed to contractually prevent manufacturers of mobile devices with an Android version *not approved by Google* from pre-installing the Google apps so highly rated by users. This *modus operandi* violates community competition law, according to the European Commission.[166]

[165] This does not change the fact that there are technical obstacles to scalability, particularly in the case of public, permissionless blockchain applications. The system is slow and costly because of the computing power required, which requires a great deal of energy.

[166] http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=1_40099

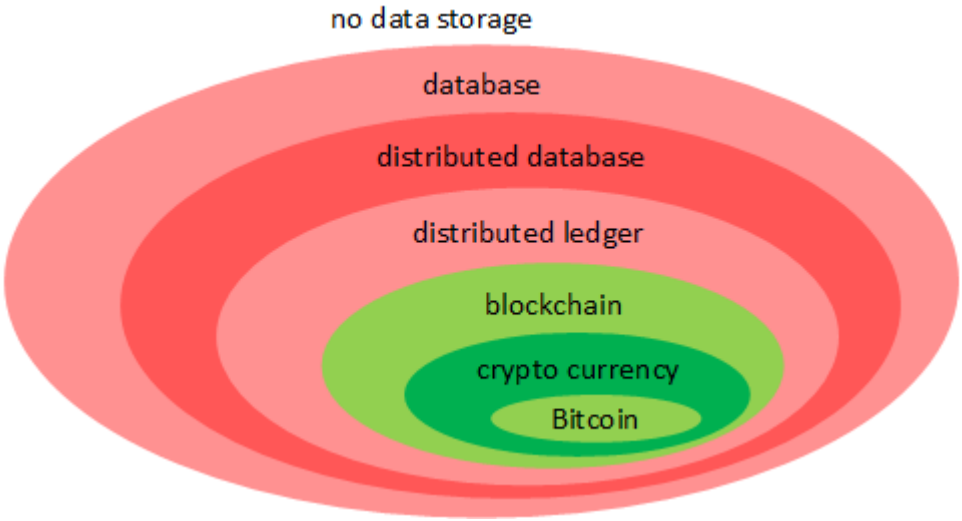
15 Technology and architecture for blockchain

Hans Nouwens & Christiaan Konstapel

It might sound familiar. A client proposes using a disruptive innovation as a solution to a business problem and immediately thinks of blockchain. Which topics is it important to discuss with the client? What important choices should be made when designing a blockchain application? In this chapter, we provide an insight into the main functions and capabilities of a blockchain and the architectural choices that can be made. We also provide an instrument to start a dialogue with the client about whether a blockchain application could be useful in a given situation, and if so, which type of blockchain could best be applied.

The structure: HOW does a blockchain work?

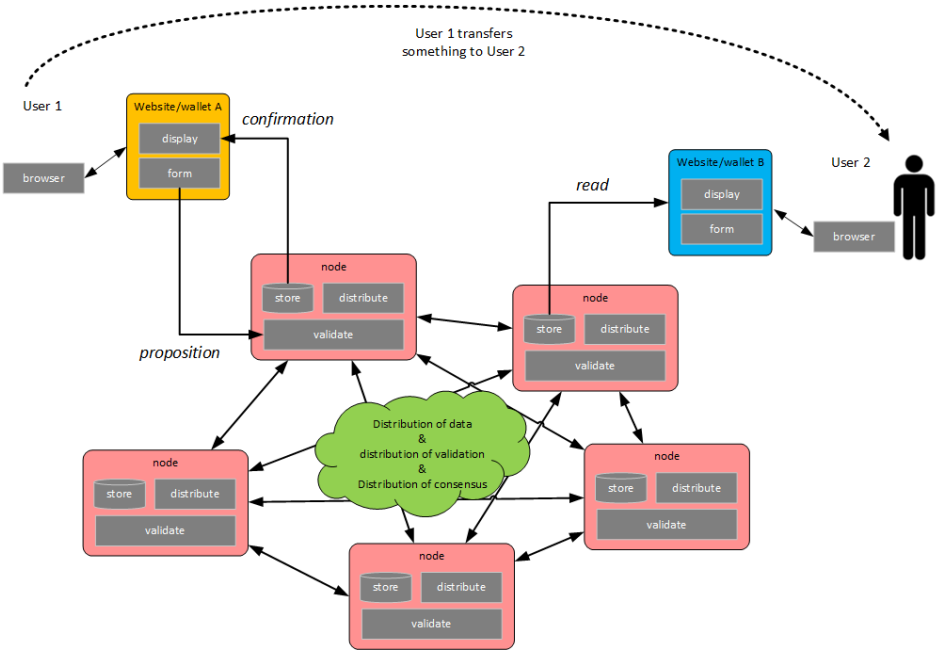
A blockchain is in essence a (specialised) form of data storage and distribution. The diagram below shows different forms of data storage, where each ring inwards shows a further specialisation of data storage.



In the simplest structure, there is an application without the storage of data. If we zoom in step-by-step to more specific forms of data storage, we see the following:

- a database, a digital collection of data;
- a distributed database, specialising in distributed data storage;
- a distributed ledger, specialising in data storage to which only transactions can be appended;
- a blockchain, a specialisation where blocks of transactions are cryptographically signed and linked in a chain;
- a cryptocurrency, a specialisation where the blocks contain transactions of currency units;
- Bitcoin, a specialisation to block transactions of the Bitcoin currency.

If we look at the technical components used in a blockchain network, we see a mix of websites and nodes. The nodes are computers that do the work. They distribute the data, validate the transactions, reach consensus and store the blockchain data.



The users do not have to trust or even to know each other to be able to do business. Trust is provided by the specialised software that runs on the nodes.

Public or private blockchains, with and without permissions

Different blockchain implementations have different types of access. Everyone can participate in a public blockchain as a user or as a node. With a private blockchain, permission is required to participate in the network as a user or a node. What participants are allowed to do can be limited by means of permissions. The process can be fine-tuned so that not everyone can see everything, or can watch but cannot append information. Any combination of public or private with and without permissions is possible.

Bitcoin is an example of a worldwide public blockchain network without permissions. Everyone around the world can join as a node, everyone can use it and there are no permissions so everyone can see everything.

Hyperledger Fabric[167] is open source software, maintained and supported by the Linux Foundation, on which a blockchain can be started. The software supports permissions. Public or private are both possible.

The functions: WHAT does a blockchain do?

The software and platforms with which blockchains are implemented are still under development. Besides the software and platforms themselves, the technical terms and the classifications that are used also differ greatly. Despite the lack of standards, a number of recurring functional building blocks can be

[167] Hyperledger fabric https://www.hyperledger.org/projects/fabric

distinguished in the various implementations. These functional building blocks can be divided into three layers: the data system, the information system and the business system. It is important to distinguish data and information.

The difference between data and information

Data is the raw bytes. Computers process data without having to know what the bytes mean. For example, there are two files on a hard disk. It doesn't matter to a computer whether it involves a photograph or a text document. The computer sees them as data and move or copy both files.

Information has meaning for a user. An image file must be viewed with different software to a text file. Merging two photographs is very different to merging two texts.

Layer 1: The data system

The functional building blocks in the data system focus on editing and storing meaningless data. These functions work independently of the meaning or content of the data and are not specific to blockchain. Enabling these functions to work together in an innovative way brings about the unique combination that we now call blockchain. The functional building blocks are:

- appending (storing) and reading data (note: no mutations and no delete);
- distributing data;
- completing and checking data with cryptographic hashes.

Many people believe that the use of cryptographic hashes makes the data unchangeable. This is not the case. *The hashes can be used to quickly determine whether the data has been changed*. The chain of hashes is broken by the smallest change. Because many nodes have their own copy of the blockchain, a majority will always be able to recognise an unauthorised mutation and reject proposed subsequent transactions.

Layer 2: The information system

The functional building blocks in the information system focus on processing and calculating with information. Data acquires a meaning in this layer. In the specific case of the Bitcoin blockchain, the meaning of the information is a cryptocoin, the Bitcoin. The functional building blocks are:

- appending and reading (transaction) information;
- sorting proposed (transaction) information;
- validating proposed (transaction) information;
- retrieving external information and storing it on the blockchain;
- obtaining a consensus;
- executing "if X and Y then Z" rules, the "smart" contracts.

A block consists of multiple information elements. Before blocks are added to the chain (the literal meaning of blockchain) the information is sorted and validated. Transferring something from Owner A to Owner B is only possible if Owner A has previously received (more of) the same from a previous owner. This sequence is essential if there are multiple transactions for one owner in one block. Consensus is achieved and a block is permanently added to the chain only if all the information is valid and each participant (node) in the blockchain network has been able to independently verify this. Once

added, blocks are no longer changed. A previous transfer can only be undone by adding a reverse transfer.

How is consensus reached in the blockchain? In order to reach a consensus with a large group of equal parties without central control, different types of consensus algorithms are used. For example, *proof-of-work, proof-of-authority, proof-of-stake* or *federated Byzantine agreement*. The purpose of these algorithms is to prevent people from breaking the rules. The proof-of-work algorithm does this by having the nodes solve such complicated cryptographic puzzles (the work) that it is not economically viable to have more than 51 percent of the computing power of the network to add fraudulent transactions. In the case of Bitcoin and Ethereum – two examples of global public blockchains – this means that an enormous amount of computing power (and therefore energy) is needed to monitor the integrity of the system.

This method of reaching a consensus is special because consensus is not achieved through human interaction and agreement but through computers. The result of this consensus is also irreversible and can, in the case of a smart contract, be carried out automatically. Confidence shifts from trust in a natural person, a legal entity or an independent third party to confidence in the software.

Layer 3: The business system

We can be relatively brief about the functional building blocks in the business system, especially because there are very few valid use cases at this level:

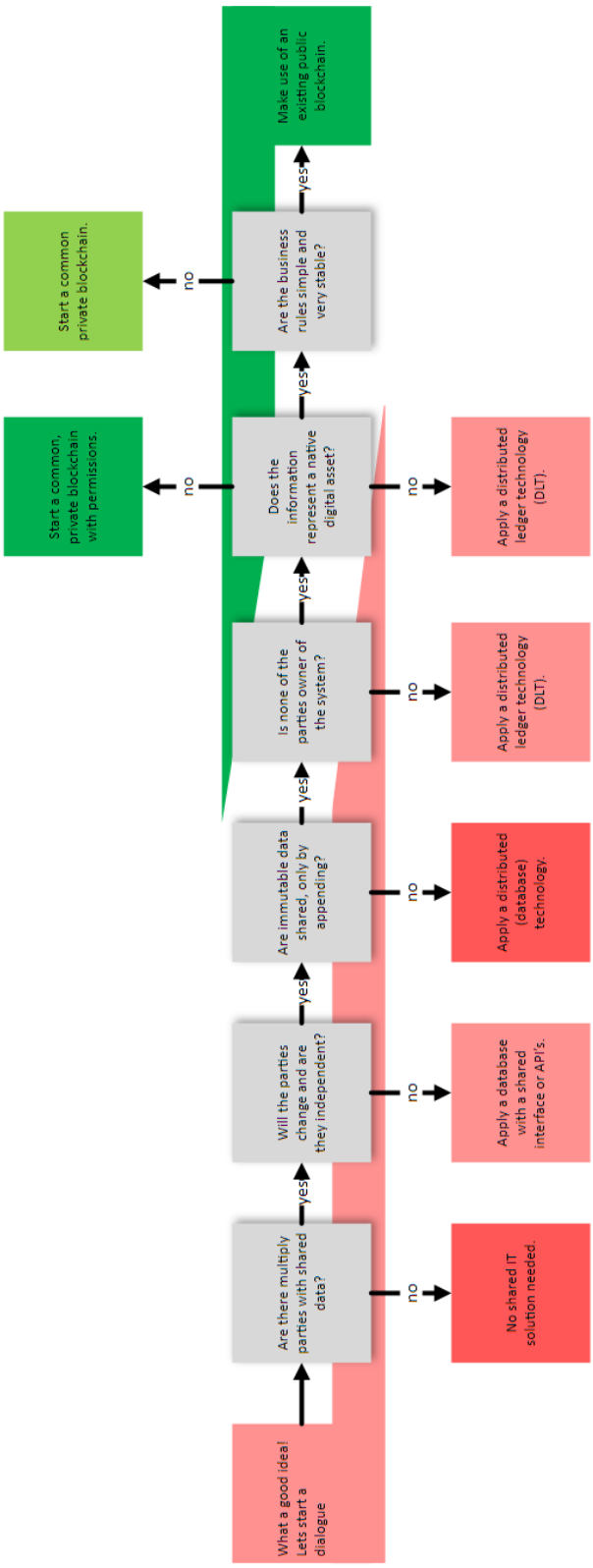
- saving and transferring digital assets;
- proving / validating a provenance.

The transfer of a (digital) asset is an example of a transaction between people supported by the (transaction) information in the previous layer. The validation of provenance is a recursive validation of ownership – for example, a list of previous owners of a painting, preferably all the way back to the artist, to prove that the work of art is not a forgery.

One of the big challenges in designing a blockchain application is the difference that exists between the real, tangible world and the digital representation in information systems. With digital data (a native digital asset) such as a licence key or a bank balance, it is possible to capture the entire genesis of the data on a blockchain. With this information, it can be assumed with a high degree of certainty that this history is 'true'. That is different for an originally physical object. Consider, for example, the purchase of a work of art. How can it be proven with sufficient certainty that the digital representation is the same as the physical work of art? Capturing information about this artwork on a blockchain does not guarantee that you are buying the real artwork; it does, however, guarantee that the accompanying (digital) papers are not tampered with.

Blockchain dialogue tool

Let us return to the conversation with the client who dreams of a blockchain application. Which questions should be asked to assess whether a blockchain could be a suitable application and if so, which type of blockchain should be chosen? The decision tree below can help. The decision tree can be used to start a dialogue with the client.



Conclusion

A blockchain is a (special) type of data storage and distribution. By adding cryptographic techniques and consensus algorithms, users can do business with each other without trusting or even knowing each other.

Points of focus for the possible use of a blockchain

- We rely on the software, but can it be trusted? Can the makers start a new version (hard fork) of the blockchain? Are there no bugs that are difficult to repair or back entrances that the developers can use for their own gain?

- The current generation of public blockchains uses a huge amount of energy to reach a consensus. Possibly an unacceptable amount of energy?

- It is not always necessary to use a complete public blockchain to solve a problem; parts of a blockchain can also add value. For example, because it is often useful to have a trusted party or parties, a higher transaction speed is required, it concerns non-digital assets or there is no economic reward for validating transactions.

- To make good decisions it is essential to consider the context – that is, the entire system. Which roles are there, and who are the users? Who controls the innovation? Which companies are no longer needed if trust can be delegated to software? Is it about digital assets or not?

Sources and references

- A Hitchhiker's Guide to Consensus Algorithms https://hackernoon.com/a-hitchhikers-guide-to-consensus-algorithms-d81aae3eb0e3
- Which Blockchain Alternative Do You Need? http://tommykoens.com/wp-content/uploads/2018/09/blockchain-alternative.pdf
- Paxos made simple https://www.microsoft.com/en-us/research/uploads/prod/2016/12/paxos-simple-Copy.pdf
- Why It's Hard to "Get" Bitcoin: The Blockchain Spectrum https://blog.unchained-capital.com/blockchain-spectrum-806847e1c575

16 Blockchain technology in the pension sector

Arnoud Reesink

The technology behind blockchain potentially has multiple applications and is opening up opportunities in many sectors. These opportunities are the result of an ambitiously constructed shared consensus network that can be used to synchronise databases. At the same time, the technology requires a complex architecture and also has other restrictions. It raises the question: where can the blockchain technology offer us something that isn't possible with our existing applications and technologies? A careful examination of the potential pros and cons of applying blockchain technology in any field is therefore of vital importance. In this chapter, we explore the possibilities and shortcomings of introducing blockchain technology in the pension sector. We first very briefly describe the characteristics of the pension system and then propose a number of ideas for implementing blockchain in the pension sector.

Characteristics of the pension sector

The current pension fund system was conceived over 50 years ago (the old-age pension has existed since 1957[168]) and is based on the labour market of that time, when most people worked full-time and rarely switched jobs. The pension sector made only limited use of standardisation. Pension schemes are complicated due to their long-term contracts and their 'legacy' from the past. The pension product has changed considerably over the years, leading to many transitional provisions. This has resulted in complex administrative systems, with the consequence that employees often only have a vague idea of their personal pension situation, not least because their influence in the system is limited.[169]

Possible implementations

Below we include two proposals for possible ways of using blockchain in the pension sector. Both of these proposals use a feature unique to blockchain known as 'smart contracts'.

Implementation 1. Standardisation

The pension system can benefit greatly from standardisation. In the context of computer science and particularly in the field of data structures, there is a term known as an 'ontology'. The term comes from ancient Greek and roughly means 'saying something about yourself'. In computer science, the term refers to a structure that describes the entities and specifications of other structures. An ontology is essentially a generic meta-model that is capable of describing all sorts of other models by filling in their attributes. [170] When we combine this concept of an ontology with the blockchain architecture, we can see how blockchain could be of benefit in the pension sector. With the use of a smart contracts-enabled blockchain platform, we can create a set of smart contracts that together construct an ontology for the administration of pensions. These smart contracts then make it possible to describe pension processes using generic definitions and formulas. The use of these definitions could potentially create standardised

[168] https://www.svb.nl/int/nl/over_the_svb/wie_zijn_we/the_historie/schemes_oud/

[169] Netspar, *Tijd for Pensionbewustzijn,* June 2015, https://www.netspar.nl/assets/uploads/007_-_Tias_Netspar_Eekelen_Rossum_Smits_Wit-1.pdf

[170] http://edepot.wur.nl/19170

ways of documenting pension processes, because every instance of a process can be described with these generic sets of rules. An ontology is an important condition for a smart-contracts blockchain to be able to work multi-client (and multi-product).

Implementation 2. Individualisation

One of the key strengths of blockchain technology is the ability to provide a single shared source of truth to a group of participants that do not necessarily have to know each other, let alone trust each other. This source of truth can host smart contracts that are in turn capable of automating contractual agreements between participants.

Using these smart contracts, it becomes possible for two entities (say an employer and employee) to set up a pension agreement directly, without the use of an intermediary that is normally responsible for the cash flow. This can lead to a structural overhaul of the pension payment system, in which the employee gains more direct control over his or her pension fund. [171] However, this does require the fundamental reform of the current (fiscal) legislation of the pension market.

The current system

In order to understand the impact of blockchain technology in this sector, it is helpful to first provide a short summary of how the current system works.

Under the current system, individual employees tend to have little choice when it comes to their pension policy. Particularly if their pension scheme is administered by a compulsory sector-based pension fund. Most of the specifics are generally decided between the 'social parties' and are limited by the possibilities offered by the pension fund (and/or its administrator) or insurance company. These parties make sure that the pension administration adheres to the legal framework. As part of his or her pension scheme, the employee can often choose a limited number of options, such as stopping work earlier or later, partial retirement or extra insurance. The money itself is handled by the pension administrator. In general, the employer and employee both pay a percentage of the employee's wage to the pension administrator in return for a claim on a future pension for the employee. Figure 1 shows this relationship between the three parties concerned. Note that the pension administrator actually has complete control over the money and that most of the decisions are made as part of the 'implementation agreement' between the employer and the pension administrator. As such, the employee only has indirect control over how his or her pension is to be built up.

[171] J, Heemskerk, *Blockchain & Pension*, June 2018

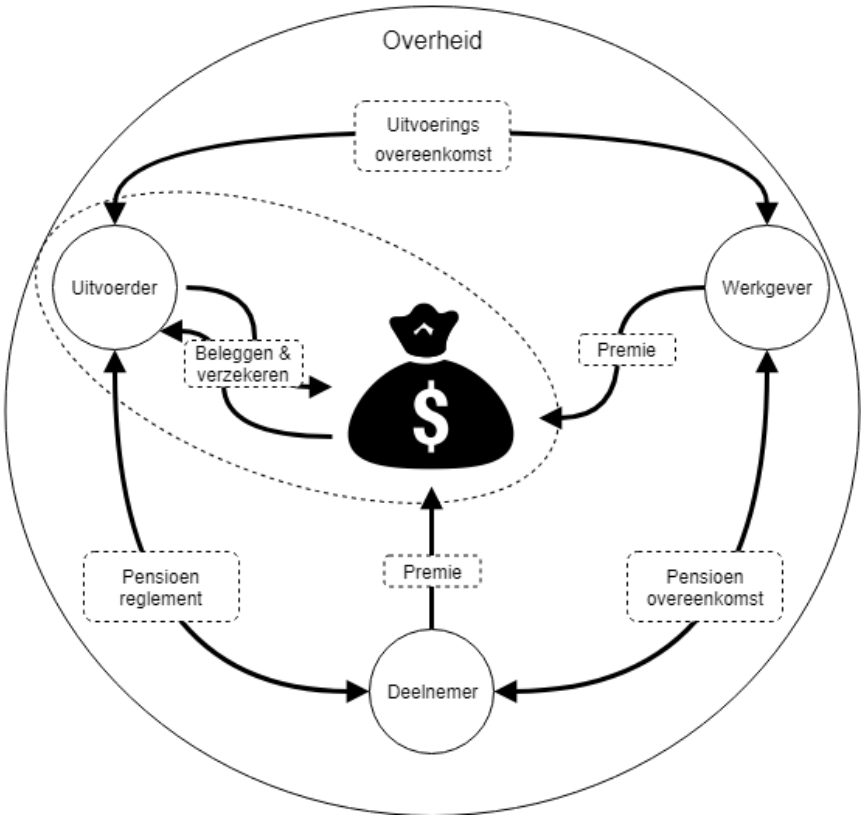


Figure 1: The current system

Structural revision

The proposed revision of this system suggests using blockchain technology in order to individualise the pension system, thereby giving users more control over their pension provisions.

In the proposed system, every employee has his or her own pension 'pot' that is located on a blockchain network. The payments are made by the employer and employee. They each fill this pot with their contribution. The money will effectively still be under the control of the employee, since the pension pot is assigned to him/her. Now, the employee can decide how and where to invest this fund by approaching the pension fund or assurance company directly. Each of these relationships is transcribed into smart contracts that are hosted on a smart contract blockchain platform.

Figure 2 displays this new relationship between the three parties. Note that (in contrast to Figure 1) in this newly proposed system the money is still under the complete control (barring legal constraints) of the employee.

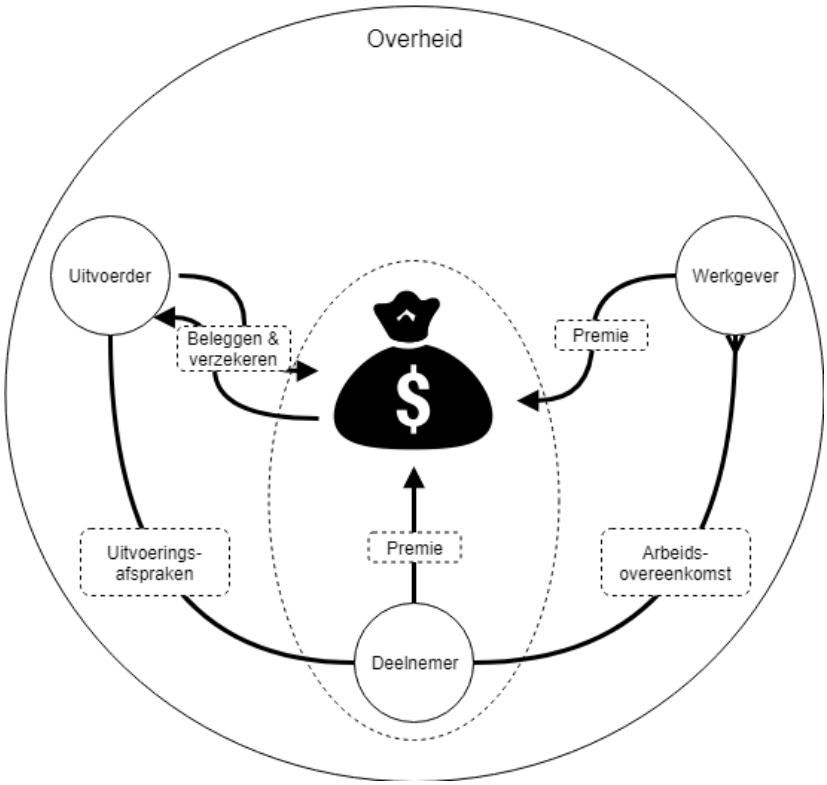


Figure 2: Proposed pension system using smart contracts

One aspect of blockchain technology is that every party involved has access to the same source of information. Because of this, the government, the insurance company/pension fund, the employer and the employee will all be in complete agreement about where the money is located and how it will be invested.

Advantages:

- This system is more transparent; people have more control over their own pension (and will therefore hopefully become 'more pension-aware').
- The system is autonomous using smart contracts, thus reducing maintenance costs.
- When employees switch jobs, they don't need to implement a value transfer; after all, the pension pot belongs to them.
- The system is accurate. Since all the information is located at a single source, everything can be retrieved in real-time.

Disadvantages:

- The current complexity of pension schemes and the variety in pension providers in the Dutch market raises the question of how to transform to a blockchain without disregarding the 'old system'. Blockchain technology is still new and (relatively) unproven. Pensions are (obviously) very future-oriented, so stability is a much more crucial requirement than in other sectors. Current blockchain implementations simply aren't yet ready to provide this type of stability.
- The current laws and regulations aren't compatible with this proposed pension system. For example, blockchain has a rusty relationship with 'Know Your Customer' information. It is difficult to save personal data on a shared ledger without revealing the identity of the persons involved.

Conclusions

Although blockchain technology in the pension sector opens up interesting possibilities, a full transformation of the pension industry into a smart-contracts blockchain, including premium intake and pay-outs, is not realistic in the near future. A more realistic introduction of this technology could be considered in the field of value transfers or asset management.

Analyses

- A pension system based on smart contracts in the blockchain is an interesting proposition. That would make the pension system more transparent, less expensive and less complicated.

- However, the complexity of the laws and regulations, the variety in pension providers on the Dutch market and the 'legacy' of the current schemes are significant obstacles to the successful and large-scale implementation of blockchain applications in the pension sector.

- The pension sector has a long-term focus and is conservative by nature. Stability and proven functionality are much more important requirements in the pension sector than in many other sectors. The large-scale adoption of a new, still relatively unproven technology in the pension sector is therefore not likely in the short term.

17 Liability in blockchains

Richella Soetens

The blockchain technology entails a great deal of security because it protects against human error and meddling with data. Things can still go wrong with a blockchain, however. The software of the blockchain can contain programming errors, for instance, the network can become deadlocked, something can go wrong in a transaction or damage can be caused by cybercrime. The decentralised nature of blockchain technology, with its many players and an international playing field, likewise entails a great deal of uncertainty in terms of liability.

Public and private blockchain

In the context of liability, the distinction between public and private blockchain is important. The public version is open to everyone, while the private blockchain only allows access to the blockchain application for a limited group of approved players. There is also a distinction between permissioned and permissionless blockchains. A permissioned blockchain has an extra authorisation layer and read and write access can differ from user to user. This enables duties and responsibilities to be allocated. It is important that behind a private and permissioned blockchain, there is an organisation that manages the blockchain, usually an alliance. A public and permissionless blockchain has no such control room. For the sake of readability, only the terms public and private blockchain are used below.

Who is liable?

Blockchain gives rise to various potential liability risks: transparency risks, cyber risks and operational risks. For instance, storing personal data in the blockchain can be in violation of privacy legislation[172], blockchain does not solve the general problem that incorrect data simply remain incorrect no matter how they are stored and there can always be errors or bugs in the blockchain software that affect the performance of the software or which make it vulnerable to attacks by hackers. If these kinds of risks occur, the question is who can be held liable.

One of the first difficulties in that context is that a blockchain involves many parties who perform different functions, such as the initiator, the programmers, miners who verify transactions, peer participants in the network and, if applicable, oracles.

The different functions entail different rights and obligations. In the event of a fraudulent transaction, for instance, the question is whether this was able to happen because of a defect in the underlying technology, in the verification, in one of the network links or because of inaccurate information added to the network by the oracle.

The more parties involved in a blockchain and the more decentralised the organisation and management of a blockchain, the more difficult it will be to point to a liable party if something goes wrong. In the event of a private blockchain with a clear governance structure, there is a greater chance, however, that responsible parties can be identified and held liable for errors that occur. It does not mean, however, that the players in an unorganised public blockchain cannot be held liable. Liability will, in that case, depend strongly, however, on the specific situation and could extend across the entire system and all participants. This entails many uncertainties and difficulties.

[172] On this, see Chapter 9 in this compilation: *Privacy and blockchain*.

Anonymity

One of the main issues in this is that the identity of most of the players (in a public blockchain) is unknown. With a public blockchain, everyone is free to participate under a pseudonym. *No identification takes place*. Consequently, the physical identity of the person or organisation managing the node and of the users remains unknown and it is possible to operate virtually anonymously.[173] Various initiatives are currently unfolding in the area of digital identification and authentication (digital identity) which could provide a solution, but these applications are still in their infancy at the moment.[174]

Applicable law and dispute resulution

In addition, because of the many players and the (often) international character of a blockchain, the question arises what regulation applies to a possible conflict and to which court the dispute should be submitted. Because the liability rules differ per country, this naturally causes a lot of uncertainty and many problems.

In order to overcome the issue of (multi)jurisdictions, and because of the specifically technical nature of blockchain, it is often argued that alternative (online) dispute resolution should be used.[175] An independent adjudicator could be designated, for instance, who would consider possible disputes within the system.[176] Decentralised dispute resolution is even considered as well, whereby the members of a blockchain community can themselves vote on a certain issue. Although these kinds of alternative mechanisms have their own challenges, they could be a wise choice because they could be used to efficiently resolve conflicts.

Decentralised autonomous organisations

The need for some formalised instrument for resolving conflicts can be illustrated with reference to the so-called *DAO hack*.[177] DAOs are decentralised autonomous organisations. DAOs are generally formed by groups of like-minded individuals with specific projects and goals in mind.

The DAO was a large crowdfunding project that ran on the Ethereum blockchain network. The DAO actually consisted of a set of smart contracts documented on the Ethereum network where they were automatically performed. From the outside, only input could be provided to the system, but the code

[173] Determining the identity of the participants in a private blockchain should, for the rest, be much less of a problem, since adequate participant identification could be more readily provided for in that. Likewise: M. van Eersel and T. van den Bergh, *Blockchain en smart contracts: toegang tot een reeks van slimme dingen [Blockchain and smart contracts: access to a series of smart things]*, no. 4, September 2017, FRP, p. 47.

[174] See, for example https://dutchblockchaincoalition.org/digital-indentities and the Smart Contract Working Group - Dutch Blockchain Coalition, *Smart contracts als specifieke toepassing van de blockchain-technologie [Smart contracts as a specific application of the blockchain technology]*, dutchblockchaincoalition.org, p. 37 and 44.

[175] Among others, see M. van Eersel and T. van den Bergh, *Blockchain en smart contracts: toegang tot een reeks van slimme dingen [Blockchain and smart contracts: access to a series of smart things]*, no. 4, September 2017, FRP, p. 47; Ibrahim Mohamed Nour Shehata, *Arbitration of smart contracts part 2 – recommendations for the future landscape of smart contracts*, Kluwer Arbitration Blog, 27 August 2018; H. Schuringa, '*Enkele civielrechtelijke aspecten van blockchain' [A few civil-law aspects of blockchain]*, Computerrecht 2017/254, p. 4.

[176] M. van Eersel en T. van den Bergh, *Blockchain en smart contracts: toegang tot een reeks van slimme dingen [Blockchain and smart contracts: access to a series of smart things]*, no. 4, September 2017, FRP, p. 47;

[177] T.J. de Graaf, *Van oud naar nieuw: van internet naar smart contracts en van mensen naar code [From old to new: from internet to smart contracts and from people to code]*, WPNR 7199-7200; T.F.E. Tjong Tjin Tai, *Smart contracts en het recht [Smart contracts and the law]*, NJB 2017/146; K. Werbach & N. Cornell, *Contracts Ex Machina*, 67 Duke Law Journal 2017, p. 30-31.

itself could not (in principle) be changed. This immediately raises questions from a legal point of view. *What is the legal status of a DAO and to what extent can DAO members be held personally responsible for the DAO's actions?* If a DAO is set up as a group of individuals, then the DAO is, in principle, nothing more than a group of individuals. There is no legal entity in the middle or that has central authority.[178] Answering these questions will therefore also depend on how the DAO is structured and the circumstances of the specific situation.

Quality problem

In *The DAO*, a defect in the programming language allowed a participant to 'empty' the portfolio of other participants. The injured parties naturally wanted these transactions reversed. Since the rules were unalterable, this was only possible, technically speaking, if the majority of the participants were to agree to make a split-off from the original code (a so-called fork). This resulted in heated debate within the Ethereum community and an ad hoc organised vote among the participants. Some of the participants refused to agree to the fork. The blockchain had to split into two communities at that point.

In order to avoid such a drastic measure, a code could be programmed such that human intervention is enabled or the code would have to contain solutions for issues that could arise. DAO developers should discuss this with the community. However, it is still difficult to determine in advance all the things that could go wrong and how to deal with them.

Hedging risks

To avoid the question of who is liable for the damage arising from, for instance, an error in the software or for a hack, it is important to contractually lay down in advance the rights and obligations of the various players (and - to the extent permitted by law - any limitations of liability). For example, in a traditional contract (use agreement), possibly in conjunction with smart contracts. This also applies for the way in which conflicts are resolved, what national law applies and to which (judicial) authority conflicts must be submitted.

Of course, making certain agreements in advance will be more feasible in the event of a private blockchain than a public one. It need not be impossible, however, to provide for matters in a public blockchain. These kinds of matters can be laid down in terms of use, for instance. In practice, there are blockchain networks that exclude their liability for a great many things in their standard terms and conditions.[179]

Other measures for professional users to anticipate possible liability could be to adopt a blockchain-related risk budget or take out insurance for potential liabilities. Insurance can be taken out for a great many liability claims. The question is whether this will also be possible (in the future) for claims relating to blockchain, however. The difficulty here is that there are not yet any best practices in this area. Time will tell whether insurers see an opportunity here and what conditions will be stipulated.[180]

---

[178] https://www.uitlegblockchain.nl/wetgeving-smart-contracts/

[179] H. Schuringa, *Enkele civielrechtelijke aspecten van blockchain*, Computerrecht 2017/254, p. 4. For an example, also see https://www.ethereum.org/agreement. Not all liability can be excluded under Dutch law, however. This is not possible for intent or gross negligence, for example.

[180] Smart Contract Working Group - Dutch Blockchain Coalition, *Smart contracts als specifieke toepassing van de blockchain-technologie [Smart contracts as a specific application of the blockchain technology]*, dutchblockchaincoalition.org, p. 38.

Conclusion

Although from a technological perspective, blockchain applications can offer more security, from a legal standpoint, risks that used to concentrate at just a few parties (or perhaps one party) are becoming spread across various participants. With all the ensuing difficulties. The use of blockchain in a closed context whereby a central authority is designated or a group of entities cooperate, can result in more legal security. At the same time, however, this would destroy a basic principle of the blockchain and particularly the public blockchain.

It seems new regulation is needed especially for public blockchains in order to adequately and above all practically provide for liability matters in relation to this new technology.

Analyses

- Because of the decentralised nature of blockchain, it is difficult to determine who can be held liable for a possible error in the blockchain. From a legal point of view, a more closed context could result in more security. The rights and obligations of the various players (and possibly limitations of liability) must also be laid down as thoroughly as possible.

- The possibility of operating under a pseudonym also makes it difficult to hold persons liable. Working with the digital identity possibilities currently being developed could provide a solution in this context.

- The decentralised and international structure of a blockchain can make it extremely difficult to determine which law applies to a conflict and to which court the dispute should be submitted. All things considered, a proper procedure for dealing with disputes is unavoidable.

- If something goes wrong, it is extremely difficult to intervene in a blockchain. The code could make human intervention possible or contain solutions for various negative scenarios.

List of authors

- M.H. Blom MSc is policy assistant for strategy and external relations at the Dutch Payments Association in Amsterdam.
- Dr. D. Dey is IT lecturer at HU University of Applied Sciences of Utrecht.
- L.M. van Ekeren MSc is marketing consultant in Vught and attached to the Weconomics Foundation as Fellow.
- N.H.A. van Duuren LLM is attorney-at-law and partner for IT, IP & Privacy at De Clercq Lawyers and Notary in Leiden/The Hague and chair of the KNVI Special Interest Group IT and Law.
- J. van Helden LLM is attorney-at-law for IT, IP & Privacy at De Clercq Lawyers and Notary in Leiden/The Hague.
- V.G. Hoek Mcs is enterprise architect at the Ministry of the Interior and Kingdom Relations in The Hague.
- E.S.R. Johan RE CISSP is Director of Soll-IT in Amsterdam and board member of the KNVI Special Interest Group IT Audit and Risk.
- C. Konstapel MSc is enterprise architect at Centric and board member of the KNVI Special Interest Group Architecture.
- J.F.K. Nienhuis BSc CISSP is information security expert in Vlissingen and secretary of the KNVI Special Interest Group Information Security and IT Security.
- H.J.P. Nouwens MSc CGEIT is enterprise architect at Sogeti and secretary of the KNVI Special Interest Group Architecture.
- V.A. de Pous LLM is independent IT lawyer and analyst in Amsterdam and co-founder and board member of the KNVI Special Interest Group IT and Law.
- A. Reesink Mcom is partner at pension consultancy bureau GroupLife in Eindhoven.
- L. Ruoff-Van Welzen is chair KNVI Special Interests Group Digital Skills, member of CEN TC 428 ICT Professionalism and Digital Skills, Director IP3 (IFIP) and director of LRWA in Voorburg.
- R. Soetens LLM is attorney-at-law IT, IP & Privacy at De Clercq Lawyers and Notary in Leiden/The Hague.
- H.L. Souw MSc RE CIPP/E is Security Officer at Nationale Nederlanden in The Hague and chair of the KNVI Special Interest Group IT Audit and Risk.
- L.L.A.M. Thissen LLM is attorney-at-law IP, IT, privacy and media law at Adelmeijer Hoyng Advocaten in Maastricht and secretary of the KNVI Special Interest Group IT and Law.
- S. Wallagh LLM is programme manager HBO-IT at HU University of Applied Sciences of Utrecht and board member of the KNVI Special Interest Group IT and Law.
- Dr. D. de Wit CMC is adviser at O&i Management Consultants in Zeist, chair of the KNVI Special Interest Group eHealth and involved in the Digital Skills in the Healthcare Sector coalition.