Trust Me: Combining Online Dispute Resolution, Law and Blockchain Technology

Tina van der Linden[*]

Abstract *This piece focuses on the unsettled relationship between online dispute resolution, law and smart contracts (and the 'trust' provided by them). It first introduces the ways in which smart contract applications on a blockchain provide the trust required to deal with unknown business partners – trust in the network rather than in an old-fashioned trusted third party. A distinction is also drawn between calculated trust and institutional trust. The piece then attempts to reconcile the trust provided by smart contracts with the demands of business and concludes that some gaps remain. Finally, it examines what online dispute resolution and the law have to offer to deal with these gaps.*

I. Introduction 454
II. Blockchain Technology and Trust. 455
III. Smart Contracts and Trust 458
IV. Trust Required to do Business. . . . 462
V. Matching Trust by Smart Contracts with Trust Required to do Business 465
VI. Filling the Gaps with Online Dispute Resolution and Law 466
VII. Conclusion. 468

I. Introduction

We require the ability to rely on other people to keep their promises and need some kind of remedy should things go wrong. Both formal and informal normative systems (law and norms, respectively, in Lessig's model)[1] provide for this trust, but they usually come with high transaction costs. Recently, technological possibilities have emerged (code, in Lessig's model) that may provide an alternate and cheaper way to create trust.

This piece examines the ways in which smart contract applications on a blockchain provide the 'trust' required to deal with unknown business partners. It first highlights the ways in which blockchain technology and

[*] Assistant Professor, Faculty of Law, Vrije Universiteit Amsterdam.

[1] Lawrence Lessig, *Code: Version 2.0* (1st edn, Basic Books 2006) 125.

smart contracts are used to create trust. Next, it discusses the nature of trust required to do business with unknown parties and determines the extent to which the two can be reconciled. Finally, it concludes that gaps remain and examines what online dispute resolution ('**ODR**') and the law have to offer as remedies to deal with these gaps.

II. Blockchain Technology and Trust

There are several excellent introductions to blockchain,[2] so we confine ourselves to the briefest possible explanation that allows for an understanding of how transacting on the blockchain creates trust by default.

Since the discovery of the internet, there has been an ongoing search for new ways to transfer money over it in a safe, anonymous and cheap fashion, and preferably, directly between the parties involved in a transaction.[3] The seminal paper by Satoshi Nakamoto[4] largely marks the end of this search. Nakamoto invented blockchain as a way to store transaction data and used it to create the first cryptocurrency – the (in)famous Bitcoin. Blockchain provides a novel way to store data and do business. Nakamoto cleverly combined existing techniques of peer-to-peer networking, asymmetric cryptography and hashing to create a revolutionary new way of bookkeeping – a distributed ledger of transaction records.

Peer-to-peer networking is a well-known alternative to the traditional 'client-server' networking model where each client's computer is connected to and dependent on a central server (and all communication passes through this central server). A peer-to-peer network instead considers computers in the network as each other's equals, or 'peers'. There is no central authority

---

[2] Mark Gates, *Blockchain: Ultimate Guide to Understanding Blockchain, Bitcoin, Cryptocurrencies, Smart Contracts and the Future of Money* (1st edn, Create Space Independent Publishing Platform 2017); Kevin Werbach, *The Blockchain and the New Architecture of Trust* (1st edn, The MIT Press 2018); De Filippi Primavera and Aaron Wright, *Blockchain and the Law: The Rule of Code* (1st edn, Harvard University Press 2018).

[3] *See*, among others, Ralph C Merkle, 'Protocols for Public Key Cryptosystems' (IEEE Symposium on Security and Privacy, Oakland, April 1980) 122 <https://ieeexplore.ieee.org/document/6233691> accessed 2 January 2020; Chaum D, 'Blind Signatures for Untraceable Payments' in Chaum D et al (eds), *Advances in Cryptology* (Springer 1983); Wei Dai, 'b-money' (1998) <http://www.weidai.com/bmoney.txt> accessed 2 January 2020; Flavio D Garcia and Jaap-Henk Hoepman, 'Off-Line Karma: A Decentralized Currency for Peer-to-peer and Grid Applications' (International Conference on Applied Cryptography and Network Security, New York, June 2005) <https://link.springer.com/chapter/10.1007/11496137_25> accessed 2 January 2020.

[4] Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2008) Bitcoin White Paper <https://bitcoin.org/bitcoin.pdf> accessed 2 January 2020.

and each computer can connect directly to every other computer. No central choking point or point of failure exists. Peer-to-peer networks are mostly popularly known for the decentralised file-sharing applications that they enabled.

Asymmetric cryptography is a technique used to encrypt and decrypt messages between two parties using two different keys, such that a message encrypted by one key can only be decrypted by the other key. The keys are mathematically related but cannot be deduced from one another. Normally, one key of the pair is called the 'private key' and should be kept strictly private. Messages encrypted by one's private key can only be decrypted by one's 'public key', which may be made available publicly. Accordingly, anyone decrypting a message with a public key can be certain that the message was sent by the holder of the corresponding private key.

Hashing is a method to seal a set of data, or, using a different metaphor, to take its fingerprint. If a hash-function is run over a set of data of any length, the output is a specific string of characters of a fixed length, called the hash. Even the minutest change in the original data set will result in a completely different hash if the hash-function is run over it again. Thus, a hash-function can be used to verify the integrity of transaction data, or in other words, to determine if any modifications have been made to said data.

A blockchain is a chain of 'blocks' of transaction data that together make up the ledger of all past transactions. The blockchain is distributed to all the peers participating in the network such that each one has an exact copy of the same ledger. Transactions concern things that can be traded on a particular blockchain, including the coin of that blockchain (like Bitcoin, Ether, or any other cryptocurrency), and possibly other things that can be represented in a digital form such as licenses, tokens, certificates and the like. The current position of each participant in the blockchain can be inferred from the ledger. To initiate a transaction, an individual must send a message containing the details of the transaction (typically, to whom they want to send what amount of money), encrypted with their private key, to the network of peers. Each one of them can verify, using the sender's public key, who the message came from. They can also determine whether or not the sender is actually entitled to the assets they want to transfer, by consulting the ledger and calculating their current position from it.

A number of verified transactions are lumped together into a new block. The new block is sealed by a hash and linked to the previous block in the chain by including the hash of this previous block in the dataset that the hash-function is run over. This process of adding new blocks to the chain

is called 'mining'. In the so-called 'proof-of-work' consensus mechanism popularly used in mining, a number (also called 'nonce', for "*number used once*") has to be determined, which when included in the data-set that the hash-function is run over, yields a hash that is below a certain threshold. This can only be done by trial-and-error – endlessly running the hash-function using random numbers as the nonce, until a nonce is found that yields a hash below the threshold.

This process makes the proof-of-work consensus mechanism extremely energy-demanding. Less energy-consuming ways of mining have been proposed,[5] but proof-of-work is still widely used. Proof-of-work can be compared to solving a Sudoku – the puzzle can be really hard to solve, but that a particular solution found is correct, is obvious. Successful miners are rewarded for the 'hard work' invested through transaction fees paid by initiators of transactions on the blockchain, and possibly, an extra amount in the coin of that particular blockchain (if so provided by that blockchain's protocol).

The fact that the hash of the previous block is included in the data which the hash-function is run over, establishes the required link. Tampering with transaction data would yield a different hash, which means that the data in all previous blocks could, for all practical purposes, be considered immutable. A change in the data would require a recalculation of all subsequent blocks because the hash value changes. A majority of the peers would need to approve of this recalculation, which is practically infeasible.[6] Alternatively, all the peers in the network would be able to see that something is wrong.

Thus, we have a distributed ledger of transactions that is immutable and requires no single controlling authority. Anyone can be a peer and verify that the approved transactions are indeed valid, and anyone can join the mining process. There is no way to rewrite history – at least not unnoticed. If we compare this with the more traditional way of processing transactions, where a bank (or another centralised institution) keeps track of each individual's position, approves and handles transactions, and remains in charge of all the administration, it is clear that the trust we invest in these intermediary 'trusted third parties' can instead be provided through blockchain networks.

---

[5] Fahad Abdullah Saleh, 'Blockchain Without Waste: Proof-of-Stake' (2020) Economics of Networks eJournal <https://www.semanticscholar.org/paper/Blockchain-Without-Waste%3A-Proof-of-Stake-Saleh/03d1b883e9d8474212094e5764646bc6450cf565?p2df> accessed 2 January 2020.

[6] Apart from the theoretical possibility of a so-called 51% attack, where an attacker manages to convince 51% of the mining nodes to validate a certain transaction, in which case it would go through.

What is described above is a so-called 'public' blockchain. There are, however, other variants. For instance, the policy by which peers are admitted to a certain blockchain may differ. If membership is restricted to a particular group, the network is termed as a 'private' or 'consortium' (permissioned) blockchain. A private blockchain can be organised in a way that best serves the purpose that the blockchain is created for – possibly, sacrificing some of the traditional public blockchain's characteristics. In particular, a central authority may re-appear – setting the rules, approving transactions (so that the energy-consuming proof-of-work mechanism can be avoided) or handling the admission of peers to the blockchain. Sacrificing the characteristics of a public blockchain comes at the price of trading the immutable trust provided by the network, as it introduces the externality of placing trust in a central authority. Nonetheless, trust may be thought of as a sliding scale – it is not a matter of all or nothing. A chain created by interlocking blocks and a ledger distributed over a reasonable number of parties may still create more trust than a central administration controlled solely by one party would, in the integrity of the data and the validity of approved transactions.

III. Smart Contracts and Trust

Smart contracts are best viewed as vending machines that 'live' on a blockchain. If you push a button and pay a specified amount of money, it gives you something in return – in case of a vending machine, a snack or a soft-drink, and in case of a smart contract, anything that can be delivered by a computer program (including ownership records, licenses, tokens, etc.) – possibly, with extended capabilities in the form of remote controlled Internet-of-Things devices (e.g., providing access to an apartment, a car, … you name it).

A smart contract is a piece of software that runs automatically on a blockchain. It may be thought of as a non-human participant that is triggered by initiating a transaction, following which its code is executed in processing the transaction, so that all the peers in the network are involved in the verification process. A smart contract may constitute a public offer that can be triggered by anyone fulfilling the conditions, or it may embody an agreement between two or more specific parties. The trust created by a smart contract is determined by the extent to which it can be relied on to be executed exactly as coded. That said, breach of contract in the sense of failure to deliver can be ruled out – once triggered, the execution of the smart contract cannot be stopped.

For smart contracts that need information from, or aim to provide an effect in the physical world (also called the 'real' world or 'off-chain' world),

an interface from and/or to the physical world is needed. In terms of trust, this interface is the most vulnerable point. Information from the real world is provided to a smart contract (inbound) by so-called Oracles, named after the function of specific priestesses in Greek mythology. Three kinds of Oracles can be distinguished:[7]

- Hardware, such as sensors and scanners,
- Software, such as information from online sources or inferences derived from data originating from other sources (e.g., a combination of sensor data and data from online sources)
- Human, such as a certification officer or an arbiter.

To understand the functions of Oracles, the following example of a mother wishing to transfer an amount of money to her son on his 18th birthday is considered. She could implement this promise through a smart contract, to make sure that no matter what, the money is transferred to the son on the date set, thus precluding her from changing her mind or the money being paid out to creditors in case of a bankruptcy. However, if the mother wants to set a condition, e.g. that the son should not have developed the habit of smoking by his 18th birthday, things become more complicated and reliance on Oracles may be required. In this context, the smart contract could provide for a number of authoritative sources that verify if the condition is met. We could think of some kind of sensor or hardware Oracle that analyses the son's breath (where the son would need to be prompted and consent to have his breath analysed), or a human Oracle – a person that can be trusted to take a decision in this matter. These options could be pre-programmed in the smart contract itself, or the matter could be left open – giving someone (either a third party or the mother herself) the authority to solve the matter. Also, a clear definition of 'the habit of smoking' is needed. What if the son shares an office with a smoker, and thus cannot help passive or secondhand smoking? Does smoking e-cigarettes, cigars or pipes count as smoking? How is smoking measured or assessed? What if the son has recently given up smoking? How much time must have passed?

If and when it is established that the son has not started smoking, he automatically receives the money pledged – there is no way to stop the transaction or change the amount. And in case it is established that he does smoke, the smart contract should ideally provide for an alternative destination for the money, for example, back to the mother or as a donation to an asthma fund.

---

[7] George Levy, 'What is a blockchain oracle?' (12 July 2018) <https://www.youtube.com/watch?v=S_1cWBWsS_I&feature=youtu.be> accessed 2 January 2020.

Another well-known example of the use of Oracles is placing a bet on the weather through a smart contract, as described, among others, by Koulu.[8] A and B place a bet on what the weather will be at a specific moment, at a specific place, by placing some money in a smart contract. Official weather reports (software Oracle) can be used to verify the weather, and the smart contract can then pay the winner. This is an illustration of how a difference of opinion between two parties may be resolved by reference to an authoritative source, and how the consequences of this solution may be executed automatically. This is very similar to how a dispute would be resolved using a smart contract application on a blockchain – which is of course what the example is meant to illustrate.

The level of trust provided by a smart contract depends considerably on the reliability of the Oracles used. In that sense, an Oracle is again a single point of failure – once the Oracle is compromised (hacked or bribed), the smart contract will be executed as coded, but on the basis of false data. Other sources of failure include damaged or out-of-order sensors and scanners, bugs in the software, incorrect or biased input data, and human error. Several approaches have been proposed to make Oracles more reliable, such as combining different kinds of Oracles, using Oracles which aggregate information from a variety of sources, or implementing the Oracle on its own consensus-based blockchain.[9]

Further, like all software, a smart contract may contain mistakes (forgivingly called 'bugs'). This may include 'normal' coding mistakes. However, it may also be the case that something went wrong in translating the parties' intentions, as expressed in natural language, into computer code. These may be problems of interpretation. It may be that there are assumptions underlying the legal text, that are not included in the code – or vice versa, that the code rests on certain unwarranted assumptions. From past attempts to build so-called legal expert systems (computer programs aimed at supporting legal reasoning), we know that the translation of law into computer code is not as

---

[8] Riikka Koulu, 'Blockchains and Online Dispute Resolution: Smart Contracts as an Alternative to Enforcement' (2016) 13(1) SCRIPTed – A Journal of Law, Technology & Society 40, 69.

[9] *See*, among others, John Adler et al, 'Astraea: A Decentralized Blockchain Oracle' (IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, August 2018) <https://www.semanticscholar.org/paper/Astraea%3A-A-Decentralized-Blockchain-Oracle-Adler-Berryhill/45f581d9c5a12f6f67956baaab71d877600e13cb> accessed 2 January 2020; John Adler, 'The State of Decentralized Oracles' (*ConsenSys Media*, 28 September 2018) <https://media.consensys.net/the-state-of-decentralized-oracles-df45bf0dc51d> accessed 2 January 2020.

straightforward as it may seem at first glance.[10] It may therefore be a good idea to include the hash of the natural language version of the contract into the smart contract itself, in order to have conclusive evidence of what the parties intentions were in normal 'legalese'.[11] This combination of a natural language version of a contract and its implementation through code is an example of a Ricardian contract.[12]

Some commercially relevant and practical examples of smart contracts include applications in container logistics,[13] identity management,[14] event ticketing,[15] participation in companies,[16] and healthcare.[17] It is easy to find many other examples of blockchain pilots and use cases. Supply chain management is a well-known use-case of smart contracts on a blockchain.[18] Say, for instance, that we want to follow the path of a box of mangos through a supply chain, all the way from the farmer who harvests the mangos to the supermarket that sells them to end-consumers. The mangos will be put in a box, and someone (a human Oracle) will need to verify that it is indeed this quantity of mangos of this quality that is inside the box. In other words,

---

[10] *See*, among others, Anne von der Lieth Gardner, *An Artificial Intelligence Approach to Legal Reasoning* (1st edn, The MIT Press 1987); Tina Smith, *Legal Expert Systems: Discussion of Theoretical Assumptions* (1st edn, Tano 1995); Mirna El Ghosh et al, 'Towards a Legal Rule-Based System Grounded on the Integration of Criminal Domain Ontology and Rules' (2017) 112 Procedia Computer Science 632; Frans H van Eemeren and Bart Verheij, 'Argumentation Theory in Formal and Computational Perspective' (2017) 4(8) The IfColog Journal of Logics and their Applications 2099.

[11] As proposed by Mattereum, *see*, 'Smart Contracts. Real Property' (2020) Mattereum Working Paper <https://mattereum.com/wp-content/uploads/2020/02/mattereum_workingpaper.pdf> accessed 2 January 2020.

[12] *See*, I Grigg, 'The Ricardian Contract' (First IEEE International Workshop on Electronic Contracting, San Diego, 2004) <https://ieeexplore.ieee.org/document/1319505> accessed 2 January 2020; Usman W Chohan, 'What Is a Ricardian Contract?' (2017) University of New South Wales Discussion Paper <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3085682> accessed 2 January 2020.

[13] Port of Rotterdam Authority, 'ABN AMRO, Samsung SDS and the Port of Rotterdam Authority are launching a container logistics blockchain pilot' (Press Release, 2018) <https://www.portofrotterdam.com/en/news-and-press-releases/abn-amro-samsung-sds-and-the-port-of-rotterdam-authority-are-launching-a> accessed 2 January 2020.

[14] *See*, 'Sovrin: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust' (2018) Sovrin Foundation White Paper <https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf> accessed 2 January 2020.

[15] *See*, 'Aventus White Paper: The Ultimate Blockchain Guide' (2020) Aventus White Paper <https://www.aventus.io/wp-content/uploads/2020/03/The-Aventus-Whitepaper-2020-.pdf> accessed 2 January 2020.

[16] *See*, 'Stem: A Blockchain Platform for the future of Capital Distribution through Private Company Shares (Security Tokens)' (2018) Stem White Paper <https://corporate-rebels.com/Blog/wp-content/uploads/2018/11/Stem-Whitepaper.pdf> accessed 2 January 2020.

[17] Peng Zhang et al, 'Chapter One - Blockchain Technology Use Cases in Healthcare' (2018) 111 Advances in Computers 1.

[18] *See*, 'Transform supply chain transparency with IBM Blockchain' (*IBM*, 18 June 2018) <https://www.ibm.com/downloads/cas/1VBZEPYL> accessed 2 January 2020.

a certificate will be produced by someone with the authority to issue such a certificate, and this certificate will be linked to the physical box (e.g. by sealing it to the box and adding a unique identifier to it), allowing it to be scanned and recorded on its journey. The box is put together with many other boxes in a container (the contents of which will also be certified and recorded), which is then shipped together with many other containers to another part of the world.

As lawyers, we are programmed to use our imagination to think of as many things as possible that may go wrong. There is always the possibility of fraud. A creepy crawler may accidentally end up in the box and eat all the mangos. The container may be blown off the ship on the high seas, the ship itself may be lost – many things may go wrong that are not necessarily recorded or prevented by the blockchain system governing the supply chain. In other words, the weakest link is the interface with the physical world, which is unpredictable and messy. The traditional issues that come with the application of abstract pre-formulated rules to subsequently arising concrete cases (such as open texture, vagueness, unforeseen circumstances etc.)[19] do not go away if smart contracts are used.

In sum, a smart contract application creates trust in the other party complying with their part of the deal as programmed. It is important to note that the weakest point is the interface to the real world (Oracles), and that all the traditional challenges of applying rules to concrete cases still remain. A blockchain cannot be considered as a single source of truth in the sense that any fact registered on the blockchain therefore, by definition, corresponds to the truth in the physical world.[20] At most, a blockchain creates trust in the peers' consensus on the truth of the facts recorded on the blockchain. There may still be a gap between the actual physical world and its representation in a database.

IV. Trust Required to do Business

We, humans, are only human. As such, we are subject to all the restrictions that come with our 'condition humaine'. We are very fragile, vulnerable and

---

[19] *See*, among others, HLA Hart, *The Concept of Law* (1st edn, OUP 1961); William Twining and David Miers, *How to Do Things with Rules* (5th edn, CUP 2014); Gardner (n 10); Smith (n 10).

[20] *See*, among others, John Plansky, Tim O'Donnel and Kimberly Richards, 'A Strategist's Guide to Blockchain' (*strategy+business*, 11 January 2016) 7 <https://www.pwc.no/no/publikasjoner/Digitalisering/sb82_A_Strategists_Guide_to_Blockchain.pdf> accessed 2 January 2020.

mortal. We have only limited rationality,[21] and face difficulty in sacrificing our own short term interest for the collective long term interest – even if such collective long term interest is also in our self-interest. This is sadly illustrated by our struggle to save our planet from our own destructive behaviour.

In order to survive, we need to cooperate. Cooperation means striking deals with others, promising to do something in exchange for a promise by the other party – you scratch my back and I'll scratch yours. Between parties that have a long term (business) relationship, keeping promises is quite evidently in their own self-interest. In other words, trust may not be a big issue. However, for one-shot transactions between parties that do not know each other, the situation is very different – how can you rely on the other party to keep their promise, if defecting is in their own short-term interest?

Our capitalist society is built on the premise that if everyone pursues their own best interest (within certain limits), everyone is better off. So, a mechanism is needed to make sure that defecting in a one-shot transaction with an unknown party is not in one's own best interest. This is, of course, where law comes in. Should someone fail to live up to their promise, you can sue them: "*See you in court!*". The law provides for remedies, in theory at least, not only in case the other party fails to meet their promises because of their own self-interest, but also if there is a misunderstanding about the agreement itself, or in cases of force majeure. In contract law, notions like (common) mistake, frustration of contract, misrepresentation etc. were developed to deal with the various things that may go wrong and to establish a fair distribution of the risks involved in trade.

However, even if a legal remedy may be available in theory, that does not always mean that it is possible or feasible to sue someone. Barriers in terms of costs, effort involved, and estimated chances of success are good reasons to accept an unfair situation instead of taking legal action. In some cases, a substitute may be available in the form of an Alternative Dispute Resolution ('**ADR**') procedure, such as arbitration or mediation. When ADR takes place online, it is usually called ODR.

Another mechanism to make sure that defecting in a one-shot transaction with an unknown party is not in one's own best interest, is reputation. Your reputation as a reliable business partner may be an important factor in other people's willingness to do business with you. The law provides mechanisms which allow you to build up a reputation (trademarks, test marks, labels) and to guard it (libel, slander). Obviously, communication is crucial

[21] Daniel Kahneman, *Thinking, Fast and Slow* (1st edn, Farrar, Straus and Giroux 2011).

for reputation to be effective as an indicator of trustworthiness. Accordingly, reviews, ratings and other public feedback and evaluation mechanisms are important but should be reliable.

Thus, we see the notion of trust arising at different points in the account above. You need to trust someone to do business with them, you need to trust the legal procedure to provide you with a fair remedy, and you need to trust reviews and ratings.

At least three different types of trust are distinguished in scholarly literature – calculative trust, personal trust, and institutional trust.[22] Of these types, both calculative and institutional trust are relevant to the decision to do business with unknown business partners.

For our purposes, calculative trust can be understood as the outcome of the comparison of the estimated profit that a transaction will bring with the risk that things will go wrong and the damage that would then arise. Institutional trust, again for our purposes, can be understood as the trust in a certain institution and/or the procedure facilitated by the institution in question. In particular, that if a legal remedy is sought, a fair trial[23] will take place, and that the subsequent decision by the court will be meaningfully enforced. Or for ODR – that the dispute is decided in a fair way (by independent and impartial jurors or arbitrators, who consider all the evidence and are open to both parties' arguments, etc.), and that the decision will be complied with (or enforced). In the institutional trust required for a legal or ODR procedure is also present an element of calculation – there are transaction costs (time involved, possibly legal advice, uncertainty about the outcome etc.) that are weighed against the estimated chances of success.

Institutional trust is also required for the process by which reviews and ratings are produced – we should be able to rely on their truthfulness and on the fact that no negative reviews and ratings were deleted by the interested party. Some intermediaries (such as booking sites) are in a position to guarantee true reviews in the sense that only those who actually booked are given the opportunity to write a review (not excluding the possibility of fake bookings in order to be able to write a favourable review). However, the transactions costs (fee paid to the booking site) perhaps outweigh the benefit of a fake review.

---

[22] Oliver E Williamson, 'Calculativeness, Trust, and Economic Organization' (1993) 36(1) The Journal of Law and Economics 453, 485-486.

[23] As expressed by Article 6 of the European Convention on Human Rights (ECHR).

Personal trust is described by Williamson to be present when one party consciously refuses to monitor the other party, is predisposed to ascribe good intentions to the other party when things go wrong, and treats him or her in a discrete structural way.[24] Given the design of the blockchain as immutable and transparent, and with its democratic consensus mechanism, the mining nodes lack the ability to act upon their personal interests – unless they are able to ally with 51% of the network. Therefore, personal trust is not relevant on a blockchain. Indeed, parties do not necessarily know (nor do they need to know) each other's identity.

In sum, the trust required to trade with unknown business partners consists in calculated trust that they will fulfill their promises and institutional trust in reputation, and in case something does go wrong, that the matter will be resolved fairly.

V. Matching Trust by Smart Contracts with Trust Required to do Business

In this section, we examine how the trust offered by smart contract applications on a blockchain provides for the trust required to trade with unknown business partners.

If indeed the trust needed to trade with unknown business partners can be provided by smart contract applications on a blockchain, this is very good news for start-ups that are yet to build up a reputation or a network of business partners. It is also good news for parties that operate from jurisdictions that do not provide a reliable or stable back-up legal structure to enforce agreements, as well as for small scale businesses or consumers/citizens that do not have easy access to (or trust in) traditional financial or government institutions. On a blockchain, it does not matter where you are located physically – at least not for the decision of others to do business with you. Blockchain based smart contracts thus have a truly enabling potential for a more equal and fair distribution of business opportunities across the globe.

The calculated trust that the other parties will fulfill their promises can to some extent be provided for by smart contract applications on a blockchain. The fact that a smart contract will perform exactly as programmed can be added to the list of things (consisting of death and taxes)[25] that you can be absolutely certain of in life. The words 'exactly as programmed' are

[24] Williamson (n 22) 483.

[25] First mentioned, reportedly, by Christopher Bullock in *The Cobbler of Preston* in 1716, and famously quoted by Benjamin Franklin in a letter to Jean-Baptiste Leroy in 1789.

crucial here, because as indicated earlier, software may contain bugs and smart contracts are no exception to this. Further, there may be differences of interpretation and cases of force majeure. In particular, the truth of facts recorded on the blockchain is limited to the consensus of the parties validating the transactions, as explained earlier. Beyond that, there is no guarantee to the actual truth. Accordingly, there is still plenty of room for things to go wrong and for conflicts to arise.

In cases where conflicts do arise, what often turns out to be crucial is what can be proven. Here, the blockchain ledger of transactions comes in very handy because there is (in theory) solid evidence of everything that happened on the blockchain. However, the solidity (and therefore, the trustworthiness) of such evidence obviously hangs together with the way the blockchain is organised. A private or consortium blockchain where only one or a few peers validate transactions, and which is not secured by a consensus mechanism specifically intended to prevent tinkering (such as proof of work), will not deserve the same amount of trust in the truthfulness of the ledger as a completely public blockchain will.

Moreover, as explained earlier, the ledger only reflects the consensus of the peers. For transactions that can be verified digitally, this is fine, but for those that have a link to events in the real world, it is important to realise that consensus of peers is not the same thing as truth in an empirical sense. Sometimes, it is claimed that an advantage of using a blockchain for recording data is that it provides a single source of truth.[26] In my view, this is misleading – a blockchain can at best provide a single source of consensus. The actual truth may be something very different.

Thus, even if we can trust a smart contract to perform exactly as programmed, there is always the possibility that something may go wrong. What is therefore required is institutional trust that in case something does go wrong (as in the examples given above), conflicts will be resolved in a fair manner.

VI. Filling the Gaps with Online Dispute Resolution and Law

Due to the possibility that something may go wrong and the corresponding need for institutional trust, it is advisable for businesses using smart contracts to incorporate appropriate dispute resolution mechanisms.

---

[26] *See*, Plansky and others (n 20) 7.

A rather straightforward way to do so is to use a so-called 'multisig arrangement' (where an action can go through if two out of three signatories approve it) in the smart contract itself, for cases in which a party's consent or approval is needed before an action can take place. For example, a contract states that the quality of goods delivered or service provided can be assessed by the recipient before a payment is made. In cases where the quality is sufficient, there would be only two parties to the agreement. If, however, the recipient finds that the quality is below standard, the signature of a third party (arbitrator) would be needed to authorise the action,[27] thereby giving the arbitrator the responsibility to assess the quality and decide on the dispute.

As discussed earlier, there is also an initiative to store (the hash of) a traditional contract in the smart contract (so that there is always evidence of the original natural-language version of the contract that the parties agree on – a so-called Ricardian contract), together with a built-in ODR mechanism, involving human arbitrators. This is the original idea of the start-up Mattereum.[28]

Additionally, there are blockchain applications that offer alternative dispute resolution, such as Kleros[29] and Aragon.[30] The idea is that the parties to a dispute (that may or may not involve blockchain transactions) use a smart contract to have independent jurors decide on their dispute. Anyone interested can apply for the position of juror – providing possible job opportunities for people who might otherwise have a difficult position on the labour market. Such a scheme can be called a Crowdsourced Online Dispute Resolution model.[31] The jurors are incentivised by game theory to look into the dispute seriously and decide either for the plaintiff or for the defendant, such that a juror who votes along with the majority gets paid in the coin of that particular application, while a juror with a minority vote loses his or her stake. From a theory of law perspective, this is a very interesting and

---

[27] Vitalik Butarin, 'Bitcoin Multisig Wallet: The Future of Bitcoin' (*Bitcoin Magazine*, 13 March 2014) <https://bitcoinmagazine.com/articles/multisig-future-bitcoin-1394686504> accessed 2 January 2020.

[28] Mattereum (n 11).

[29] Clément Lesaege, Federico Ast, and William George, 'Kleros Short Paper v1.0.7' (2019) Kleros White Paper <https://kleros.io/static/whitepaper_en-8bd3a0480b-45c39899787e17049ded26.pdf> accessed 2 January 2020.

[30] 'Aragon Network' (2019) Aragon White Paper <https://github.com/aragon/whitepaper> accessed 2 January 2020.

[31] *See*, for a proposal of a model for fair Crowdsourced Online Dispute Resolution (CODR), Daniel Dimov, 'Crowd sourced Online Dispute Resolution' (PhD thesis, Leiden University Center for Law and Digital Technologies 2017) 149-166 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3003815> accessed 2 January 2020. It is not at all clear how Kleros or Aragon comply with the elements identified here for a fair CODR procedure.

not uncontroversial way to look at adjudication. Jurors, thus incentivised, will vote for what they think the majority of jurors will vote for. This is not necessarily the 'right' answer,[32] or the most just answer. Take for example a case where the most just answer is not evident from a quick glance at the case, and which instead requires an active effort to look at all the details, weigh up the interests etc.

How can a juror in such situation be confident that all the other jurors put in the effort of really looking into the case? It may very well be that their safest bet (just like everyone else's) is to go for the quick solution, and that may not be the most just.

Finally, if all else fails, we always have good-old law to fall back on. Everyone is entitled in full equality to a fair and public hearing by an independent and impartial tribunal, in the determination of his rights and obligations, according to Article 10 of the Universal Declaration of Human Rights.[33] Of course, there may be hurdles to sue a party located in a different jurisdiction, but private international law does provide for solutions, at least in theory.

Blockchain applications do not operate in a legal vacuum.[34] Like internet mediated communication, blockchain applications concern real people in the real world with real assets. At the interface between blockchain and the real world, so at the exchanges, where cryptocurrencies are spent or where the effects of smart contracts materialise, the long arm of the law may appear, and seize, tax, protect or enforce as it sees fit. And that is as it should be, because the law exists for a reason.

VII. Conclusion

The relationship between trust, blockchain, ODR and law is still rather confusing and needs further attention and study.

It seems clear that blockchain can organise trust in a new and different way, and that this may have far-reaching consequences. Some business

---

[32] If a single right answer exists at all, which is not uncontroversial. *See*, the discussion between Hart and Dworkin in Hart (n 19) and Ronald Dworkin, *Taking Rights Seriously* (5th edn, Harvard University Press 1978). Also discussed, among others, in Richard Bellamy, 'Ronald Dworkin, Taking Rights Seriously' in Jacob T Levy (ed), *The Oxford Handbook of Classics in Contemporary Political Theory* (OUP 2015).

[33] In the determination of his civil rights and obligations, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law (ECHR, art 6).

[34] *See*, for a detailed account on the relation between blockchain and law, Werbach (n 2).

models will become outdated, and other business opportunities will arise. Traditional trusted third parties like banks and public notaries may need to reinvent themselves and find new ways in which they can offer added value, now that the trust they used to deliver can be provided by blockchain-based applications. However, there remain certain shortcomings – the trust provided by smart contracts needs to be complemented by the availability of legal/institutional procedures to fall back on. The availability of an ODR option may enhance trust in blockchain based applications, and ODR may itself be organised as a smart contract – solving the issue of compliance with the decision. It could also be argued that smart contracts prevent disputes to some extent (thus partly putting both ODR and law out of a job), because automatic execution serves to disincentivise breach of contract.

It seems equally clear that the law will need to evolve and develop itself, but that we cannot do without law in the foreseeable future. ODR and law can be seen to complement each other – for cases where the recourse provided by law is inefficient or even inaccessible, ODR may provide a useful solution. Blockchain also needs law – in order to inspire trust, there must be governance and compliance with the existing legal order.

Trust, therefore, is what we all need in order to be able to cooperate and to survive. I can see it in my puppy's eyes.