Is a ‘smart contract’ really a smart idea? Insights from a legal perspective

Article *in* Computer Law & Security Review · June 2017

DOI: 10.1016/j.clsr.2017.05.007

Mark Giancaspro
University of Adelaide
39 PUBLICATIONS 274 CITATIONS

Is a 'Smart Contract' Really a Smart Idea? Insights from a Legal Perspective

Mark Giancaspro[a]

Swift developments in the emerging field of blockchain technology have facilitated the birth of 'smart contracts': computerised transaction protocols which autonomously execute the terms of a contract. Smart contracts are disintermediated and generally transparent in nature, offering the promise of increased commercial efficiency, lower transaction and legal costs, and anonymous transacting. The business world is actively investigating the use of blockchain technology for various commercial purposes. Whilst questions surround the security and reliability of this technology, and the negative impact it may have upon traditional intermediaries, there are equally significant concerns that smart contracts will encounter considerable difficulty adapting to current legal frameworks regulating contracts across jurisdictions. This article considers the potential issues with legal and practical enforceability that arise from the use of smart contracts within both civil and common law jurisdictions.

KEYWORDS: Smart – Contract – Law – Enforceability – Blockchain – Technology – Computer – Program – Intermediary – Ledger

1. Introduction

As long ago as 1994, American computer scientist Nick Szabo proposed what was then a fanciful notion of 'smart contracts'; computerised transaction protocols which execute the terms of a contract.[1] At that point in time, the existing economic and communications infrastructure was insufficient to support such protocols.[2] Today, the requisite infrastructure is available and smart contracts are increasingly being developed, tested and implemented across a variety of industries the world over. This enthusiasm is unsurprising; smart contracts conceivably offer the promise of more efficient and cost-effective transactions which remove the heavy dependence upon traditional intermediaries (such as banks and credit companies). However, the use of smart contracts also gives rise to a number of legal issues, along with practical concerns as to functionality, security and workforce impact.

This article contributes to the small body of literature addressing the concept of smart contracts by considering the legal issues that do or may arise from their use. It begins by briefly introducing the

[a] LLB (Hons.), LP, PhD. Lecturer, Law School, University of Adelaide.

[1] Don Tapscott and Alex Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business and the World* (Penguin, 2016).

[2] Steve Omohundro, 'Cryptocurrencies, Smart Contracts, and Artificial Intelligence' (2014) 1(1) *AI Matters* 19, 19.

reader to blockchain and distributed ledger technology, and smart contracts generally. It then proceeds to examine in detail the principal legal issues arising from the use of smart contracts, focussing upon actual and potential conflicts with established principles of contract law. For comparative purposes, the position under Australian contract law is measured against those in England, France and the United States. Finally, the article concludes by cautiously welcoming the dawn of smart contracts but foretelling of potential difficulties that lie ahead for commercial parties and lawmakers.

2. Blockchain Technology and Smart Contracts

Szabo's notion of smart contracting attained greater attention following the publication of his seminal paper 'The Idea of Smart Contracts' in 1997. In this paper, Szabo identified a purchase from a humble vending machine as a primitive form of 'smart contract' in that it involved the autonomous transfer of ownership of property, such as a confectionary item or can of drink, upon receipt of predetermined input (i.e. money). Szabo also described a number of potential applications of smart contracts including the automated transfer of digital property (such as shares) upon the occurrence of a specified event; motor vehicle immobilisation (where the vehicle would not operate unless the security protocols stipulated in the contract were satisfied); and peer-to-peer property lending (where lent property would revert to the lender if the borrower defaulted on specified conditions). Thanks largely to the advent of cryptocurrency platforms such as Bitcoin and Ethereum, these applications and many others are now possible. To understand how, one must have a basic understanding of how a 'smart contract' actually operates.

As was mentioned a brief moment ago, smart contracts are constructed upon an underlying cryptocurrency platform. A cryptocurrency is essentially 'a decentralised system for interacting with virtual money in a shared global ledger'.[3] That ledger is the 'blockchain', so called because the transactions chronologically recorded within it by a network of computers are grouped into blocks.[4] 'Miners', the name given to participants within the blockchain, can create smart contracts by posting a transaction to that blockchain. A unique feature of this arrangement is that the transactions are not validated by any central authority or trusted intermediary; rather, all transactions are validated through a series of cryptographic screening procedures.[5] As such, the blockchain network is transparent in

[3] Kevin Delmolino, Mitchell Arnett, Ahmed Kosba, Andrew Miller and Elaine Shi, 'Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab' (18 November 2015) University of Maryland, p 2. Available at https://eprint.iacr.org/2015/460.pdf.

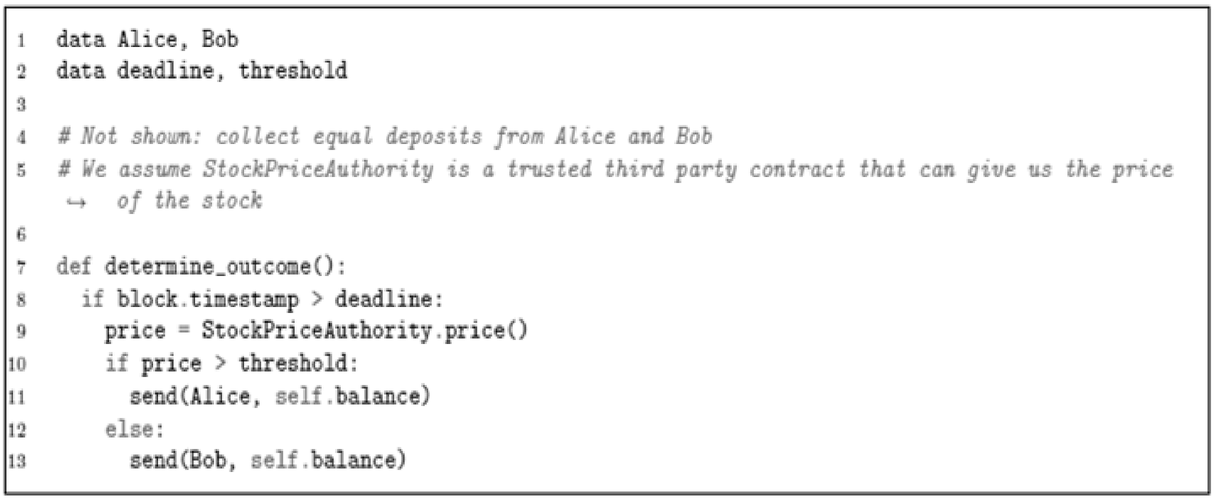
[4] Gareth W Peters and Efstathios Panayi, 'Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money' in Paolo Tasca et al (eds), *Banking Beyond Banks and Money: A Guide to Banking Services in the Twenty-First Century* (Springer, 2016) 239, 242.

[5] Two of the leading cryptocurrencies, Bitcoin and Ethereum, for example, utilise 'proof-of-work' protocols to authenticate transactions. These protocols involve the miner solving various cryptographic problems which, when satisfied, allows the transaction to be coded to the blockchain.

nature and visible to all users within the network. Once authenticated through consensus of network users, the transactions are then coded with algorithms before being added to the blockchain (which are later decoded to produce the specified data) and timestamped. Blockchain technology is essentially, therefore, a form of Distributed Ledger Technology (DLT).

Fundamentally, a smart contract is a computer program which verifies and executes its terms upon the occurrence of predetermined events. Once coded and entered into the blockchain, the contract cannot be changed and operates in accordance with its programmed instructions.[6] Delmolino, Arnett, Kosba, Miller and Shi provide a useful and simplified example of a smart contract and how it might be coded to accomplish its purpose.[7] In this example, two parties – Alice and Bob – engage in a speculative financial swap. The parties each deposit equal amounts of the designated cryptocurrency before making opposing bets as to the price of a stock on an exchange at some point in the future. Alice believes the stock will be higher than an estimate provided whereas Bob thinks it will be lower.

When the deadline arrives, the stock price is queried by reference to some external pricing authority (say the relevant stock exchange itself, reference to which is coded into the smart contract). Depending on the stock price at that point in time, either Alice or Bob receives the entire sum of money jointly wagered. Delmolino, Arnett, Kosba, Miller and Shi provide a graphic representation of the coding thus:



```
data Alice, Bob
data deadline, threshold

# Not shown: collect equal deposits from Alice and Bob
# We assume StockPriceAuthority is a trusted third party contract that can give us the price
 ↪  of the stock

def determine_outcome():
  if block.timestamp > deadline:
    price = StockPriceAuthority.price()
    if price > threshold:
      send(Alice, self.balance)
    else:
      send(Bob, self.balance)
```

It can be seen that this smart contract provides for the identities of the parties, the deadline for reference to the exchange price of the stock wagered on, the precondition, and the logic for execution of the program and determination of the outcome as framed by the precondition. This is but one

[6] As will be discussed later in the article, this is one of several practical difficulties which stem from the use of smart contracts.

[7] Delmolino, Arnett, Kosba, Miller and Shi, above n 3, pp 4-5.

small-scale example of how smart contracts might be used to facilitate a wide number of transactions, financial or otherwise. As will be discussed later in the article, the potential of blockchain technology is only now starting to be realised and seized upon.

Blockchain technology enables such contracts to operate efficiently by providing a simple, cost-effective mechanism for the secure control and transfer of digital property without the use of – or, perhaps more accurately, with reduced dependence upon – intermediaries, and with the added advantage of transparency stemming from decentralisation of data. Prior to the development of blockchain technology, smart contracts could not feasibly operate. Within the last decade, however, significant developments in this field have broadened the possibilities and heavy investment into, and experimentation with, blockchain (distributed ledger) technology is now occurring.[8]

There are obvious advantages to using smart contracts. For one, they offer the promise of *increased efficiency*. Transactions facilitated through smart contracts operating on a blockchain are not validated by a trusted intermediary but by consensus of the network's users. Rather than a bank, credit provider, insurance company or the like enabling the digital transfer of property on the terms of the agreement, the coding of the smart contract does all of the work autonomously (once the transaction has been verified through the completion of cryptographic protocols). The miners on the blockchain – the contract parties – need only decide upon the content of their agreement and the contract effectively executes itself. This process of disintermediation improves efficiency by allowing the blockchain to address all critical aspects of the transaction from record-keeping to auditing, monitoring and enforcement.[9] Subsequently, settlements can take place in far quicker time given that there is no significant period of delay during which a traditional intermediary would authorise and process the transaction. Transfers occurring on the blockchain are instant. With further refinement of distributed ledger technology and smart programming, instantaneous settlement for even the most complex of transactions becomes a very real prospect. Moreover, automating a number of key processes during the life of a contract translates to reduced human involvement; if 'fewer hands' are required to create and fulfil a contract, efficiency is likely to be improved.

Smart contracts may also result in *reduced transaction and legal costs*. The absence of any central authority or trusted intermediary in a blockchain, and the manner in which blocks of transactions are openly verified and added to the chain by its miners, means that many of the numerous transaction and legal costs that would normally be incurred through intermediated transactions are removed. Such fees are typically in the nature of service or administration fees, or legal costs associated with the

[8] In November 2016, it was reported that USD $1.4 billion had been invested in blockchain start-ups in 2016 alone. See https://news.bitcoin.com/1-4-billion-invested-blockchain-pwc/.
[9] Brydon Wang, 'Blockchain and the Law' (2016) 19(1) *Internet Law Bulletin* 246, 252.

preparation, supervision and execution of written contracts. A common example is a contract formed via credit card purchase: a consumer purchases an item from a merchant and pays via credit card; the merchant then applies a surcharge (said to represent the cost to the merchant of accepting payment by credit card); the credit card company similarly applies its fees. All of these costs are entirely avoidable through the use of a blockchain.[10] The potential cost savings from utilising smart contracts are not limited to the transactions themselves; given their relative simplicity, they are likely to significantly reduce infrastructure costs.[11] Proverbially 'cutting out the middle man' through the use of smart contracts is therefore a means for businesses, governments and consumers to potentially dramatically reduce operational and commercial expenses. A consequential advantage of this reduction in overheads is that the bar of entry for users is lowered.[12]

A final opportunity presented by smart contracts is greater *transparency and anonymity*. With the decentralisation of data through distributed ledgers such as blockchains comes greater transparency. The lack of a central authority or trusted intermediary validating and collating all transactions, and the transparent nature of the blockchain, means commercial arrangements conducted through smart contracts within a public (unpermissioned) ledger are visible to all miners. With this transparency comes greater confidence that one user can trust another. Miners also benefit from anonymity the kind of which they would not enjoy in conventional commercial transactions. For example, trusted intermediaries who facilitate many common sales agreements, such as credit card companies, require proof of identity before a promise of future payment will be accepted and processed. As such, these intermediaries store vast amounts of critically sensitive information personal to each consumer who employs their services. This places them at risk of exploitation through theft. In April 2016, for example, the Australian version of popular online shopping site Gumtree – owned by online auction giant eBay – was hacked, with many users' personal data being unlawfully accessed.[13] Transactions utilising cryptocurrencies allow consumers to purchase items in an online environment without having to provide their personal information.

[10] There will, of course, be costs associated with participation on the blockchain network for such things as computational power. There may also be some minor fees associated with specific transactions. Overall, however, transactions completed through smart contracts on the blockchain will almost certainly be far cheaper than conventional intermediated transactions.

[11] Of course initial development and implementation of the computational infrastructure necessary to support blockchains will attract costs. Those transition costs will, however, be offset by the significant long-term savings enjoyed as a consequence of disintermediation. An interesting contrasting view is provided by Angela Walch, who argues that the various risks associated with blockchain technology make it an unsuitable basis for financial market infrastructure and that it might end up costing just as much or even more to accommodate or rectify any operational issues that arise: Angela Walch, 'The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk' (2015) 18 *Legislation and Public Policy* 837.

[12] Delmolino, Arnett, Kosba, Miller and Shi, above n 3, p 1.

[13] Jennifer Dudley-Nicholson, 'Australian Gumtree Users Targeted in Hacking Attack, with Personal Details Stolen' (*News.com.au*, 29 April 2016) <http://www.news.com.au/technology/australian-gumtree-users-targeted-in-hacking-attack-with-personal-details-stolen/news-story/56034ebce5c54a0d21aa4d5bce711ed2>.

A smart contract might be programmed to purchase a particular item at a certain price and on the assurance that consumer guarantees and warranties are included. Rather than the vendor being connected to the purchaser's personal and financial information via a trusted intermediary, they are connected directly to the purchaser's digital 'wallet'[14] meaning that the purchaser's identity is never released. Indeed, as Fairfield notes, 'depending on the nature of the transaction and the need for shipping addresses, it is entirely possible that the [smart contract] can buy and sell on the consumer's behalf without providing any information about the consumer to the [vendor] at all'.[15]

3. Smart Contracts and Compatibility with Contract Law

Having briefly discussed the concept of blockchain technology and smart contracts, and canvassed some of the principal advantages stemming from their use, this article now turns to considering perhaps the most vexing of issues with respect to smart contracts: how the existing law of contract will adapt to regulate and enforce these creatures of blockchain technology. Whilst it would be easy to assume that smart contracts would be treated like any other contract in this regard, a brief consideration of their unique nature and of the various established principles of contract law demonstrates that there are likely to be some theoretical and practical difficulties and inconsistencies. A selection of contract doctrines and principles will be discussed to provide context. For comparative purposes, the position under Australian contract law will be measured against those in England,[16] France,[17] and the United States.[18]

3.1 Establishing Capacity

Contractual capacity refers to a party's ability to enter into a contract. Generally speaking, under Australian and English law, a minor – being someone under the age of 18 – cannot enter into a contract as they lack capacity.[19] The position is the same in the United States[20] and France.[21] Under

[14] A digital wallet is an electronic device which allows an individual to make electronic transactions. Digital wallets come in various forms, a common example of which is contactless payment technology embedded into smartphones whereby a person can pay for a good or service by bringing their device into close proximity of the other party's designated payment point. See further: Rajesh Krishna Balan and Narayan Ramasubbu, 'The Digital Wallet: Opportunities and Prototypes' (2009) 42(4) *IEEE Computer* 100; Richard Kemp, 'Mobile Payments: Current and Emerging Regulatory and Contracting Issues' (2013) 29(2) *Computer Law & Security Review* 175.

[15] Joshua A T Fairfield, 'Smart Contracts, Bitcoin Bots, and Consumer Protection' (2014) 71(2) *Washington and Lee Law Review Online* 35, 46.

[16] Founding nation of the common law system.

[17] Civil law nation.

[18] Hybrid common law and civil law nation.

[19] All Australian jurisdictions define a minor as a person under the age of 18 years: *Age of Majority Act 1974* (ACT); *Minors (Property and Contracts) Act 1970* (NSW); *Age of Majority Act (NT)*; *Law Reform Act 1995* (Qld); *Age of Majority (Reduction) Act 1971* (SA); *Age of Majority Act 1973* (Tas); *Age of Majority Act 1977* (Vic); *Age of Majority Act 1972* (WA). The United Kingdom ratified the *United Nations Convention on the*

Australian and English law there are limited exceptions to the rule that a minor cannot contract; they may, for example, enter into contracts for 'necessaries' (being goods or services needed to maintain the minor in his or her status or condition).[22] In all other cases, the contract is generally voidable at the minor's election.[23]

Given that the parties to a smart contract may, and indeed often will, be unknown to one another, there is a very real risk that a party who has attained the age of majority may inadvertently contract with a minor cloaked by the anonymity of the internet. This threatens the enforceability of the agreement. Elaborate screening procedures to determine age prior to entry of a transaction onto a blockchain may be required though these are likely to be difficult to police. Moreover, whether or not such a contract would be binding would depend upon the jurisdiction(s) in which it was formed and, in the case of common law countries, whether the contract was one falling into one of the excepted 'classes' of contract (such as one for necessaries). Whether a contract was one for necessaries or not would rely upon analysis of the subject matter. It is dubious to suggest that a purchase of a cryptocurrency, for example, is one of necessaries given that it is, on its face, not vital to the minor's sustainment.

3.2 Contracting Under Mistake

A related issue is where a party contracts with another party on the assumption that the other party is who they say they are, when in actual fact they are someone else. In the online context, this would be relevant where a hacker had assumed someone's digital identity and misappropriated their cybercurrency. Under Australian and English law, where parties do not contract face to face, and where one of the parties to the agreement is mistaken as to the identity of the other party at the time of entry into the agreement, the contract is void at common law.[24] Under French law, the position is slightly different: the doctrine of mistake *can* nullify an agreement where the mistake affects the very

Rights of the Child in 1991. The Convention defines a child (minor) as being a person under 18 years of age, unless an earlier age of majority is recognised by a country's law. As such, a minor in English law is also someone under 18 years. Historically, the position at common law has differed, with the age of majority previously being as high as 21 years.

[20] All but three US states stipulate 18 years as the age of majority, the exceptions being Alabama (19), Nebraska (19) and Mississippi (21).

[21] This is reflected in various provisions throughout the French Civil Code (*Code Civil des Français 1804*), as amended.

[22] *Chapple v Cooper* (1844) 13 M & W 252; 153 ER 105.

[23] The position is the same in the United States: see *Restatement (Second) of Contracts* (1981) art 14; *Casey v Kastel* 237 NY 305 (1924). It is also similar in France where such a contract may be rescinded pursuant to art 1305 of the Civil Code: see generally John Bell, Sophie Boyron and Simon Whittaker, *Principles of French Law* (Oxford University Press, 1998) p 425.

[24] *Cundy v Lindsay* (1878) 3 App Cas 459; *Shogun Finance Ltd v Hudson* [2003] UKHL 62. This is known as 'unilateral mistake'.

substance of the agreement.[25] In the US, a contract may generally be voidable at the mistaken party's option where the other party was aware of the mistake (which would always be the case in situations of identity fraud) and enforcement of the contract would be unconscionable.[26]

Given the potential ease with which financial theft and identity fraud can be committed through digital technologies, there is a real risk that many transactions facilitated through smart contracts may be struck down for want of legal enforceability. The capacity for computers to amplify the scope of such contracts and potentially engage millions of consumers at a time across many jurisdictions (in contrast somewhat to traditional non-digital contracts) means that the process of compensating the innocent parties and penalising the offenders will be incredibly arduous.

Even assuming that a smart contract had been formed between two or more legitimate parties, who would be responsible if a smart contract endured a coding error resulting in losses to one or more of the parties? Paper contracts or even those reduced to writing in digital form (i.e. in word documents stored on computer) cannot simply amend themselves. Theoretically, however, a smart contract's code *could* spontaneously change and thereby affect its manner of operation. Liability cannot logically be assigned to either party in this instance, or in the related situations that the error was caused by a third party – either the programmer incorrectly coding the terms agreed by the parties, or an external information source from which the contract draws variable information.[27] One solution might be to assume that the smart contract has been frustrated by virtue of the fact it has without fault of either party become impossible to perform as originally envisaged.[28] In that event, the contract would be rescinded in its entirety and the parties would be relieved of any future obligations. Again, however, spontaneous corruption of content is a risk that is entirely absent in the case of traditional non-digital contracts.

3.3 Formation via Technology – When Do the Offer and Acceptance Occur?

Under Australian and English law, an offer is characterised by a party's indication of willingness to be bound by the terms of a promise he or she has made to another party, with the latter being provided

[25] French Civil Code, art 1110.

[26] *Restatement (Second) of Contracts* (1981) art 153; *Gethsemane Lutheran Church v Zacho* 258 Minn 438 (1960)*; Maryland Casualty Co v Krasnek* 174 So 2d 541 (1965).

[27] Some examples of such a contract are provided later in this article (at 3.7) when interpretation of contractual content is considered.

[28] This is the fundamental rationale behind the doctrine of frustration. See in England/Australia: *David Contractors Ltd v Fareham Urban District Council* [1956] AC 696; *Codelfa Construction Pty Ltd v State Railway Authority of New South Wales* (1982) 149 CLR 337. In the US: *Restatement (Second) of Contracts* (1981) art 265; *Uniform Commercial Code* (UCC) arts 2-613–2-615; In France: French Civil Code, art 1147.

with the opportunity to elect between acceptance and rejection of the proposal.[29] Unequivocal assent to the offer then confirms that it has been formally accepted and that a 'meeting of the minds' has occurred. The *Uniform Commercial Code* (US) similarly states that 'an offer to make a contract shall be construed as inviting acceptance in any manner and by any medium reasonable in the circumstances'.[30] In French law, it is essential to establish consent to contract through a 'meeting of the minds' – the *accord de volontés* – by identifying an offer by one party to do (or not to do) something as well as a corresponding acceptance.[31]

In traditional contracting, i.e. contracting which does not occur exclusively via technology, it is relatively straightforward to identify when an offer has been made and accepted by examining the words and conduct of the parties along with all relevant circumstances. The only anomalous exception in this regard is where acceptance is sent via post, in which case the acceptance is deemed effective as soon as it is posted as opposed to when it is received by the offeror (commonly known as the 'postal acceptance rule' or 'mailbox rule').[32] The analysis is made more difficult, however, when an offer to contract is made and ostensibly accepted via *technology*. In such situations, given the instantaneous nature of technologies such as email and text messaging, uncertainty surrounds the point at which 'acceptance' is deemed to have occurred.

The position in England and Australia is that the postal acceptance rule does not apply to instantaneous forms of communication such as telephone and facsimile[33] and, in Australia at least, transactions occurring via the internet (such as email) have been judicially regarded as analogous to telexes.[34] Consequently, acceptance is effective upon *receipt*, as opposed to at the time of *dispatch*, as would be the case under the postal acceptance rule.[35] England appears to endorse a similar approach through reg 11 of the *Electronic Commerce (EC Directive) Regulations 2002*, which provides that communications 'will be deemed to be received when the parties to whom they are addressed are able to access them'. French law is silent on this issue and the French courts have typically decided such questions on a case-by-case basis.[36] In the US, the prevailing view is that acceptance is generally deemed to have occurred once dispatched,[37] even where this occurs via the internet.[38]

[29] *Stover v Manchester City Council* [1974] 1 WLR 1403; *Brambles Holdings Ltd v Bathurst City Council* (2001) 53 NSWLR 153.
[30] *Uniform Commercial Code* (UCC) art 2-206.
[31] French Civil Code, arts 1101, 1106.
[32] *Adams v Lindsell* (1818) 106 ER 250.
[33] *Entores v Miles Far Eastern Corp* [1955] 2 QB 327; *Brinkibon Ltd v Stahag Stahl und Stahlwarenhandelsgesellschaft mbH* [1983] 2 AC 34.
[34] See *Olivaylle Pty Ltd v Flottweg GMBH & Co KGAA (No 4)* (2009) 255 ALR 632.
[35] This position appears to be reflected in the provisions of the *Electronic Transactions Act 1999* (Cth). See for example s 14A.
[36] Commission on European Contract Law, *Principles of European Contract Law* (Kluwer Law International, 2000) p 173. Bell, Boyron and Whittaker note that there seems to be a preference amongst the French courts for

Assume, then, that a smart contract for the sale of goods was being negotiated between two parties. Typically, smart contracts are initiated by messages sent using public-key infrastructure (PKI) through an internet connection, in similar manner to emails.[39] It would become necessary, in this situation, to determine whether an offer had been validly made and accepted. The obvious question is whether acceptance occurs once the party seeking to purchase the goods transmits their offer, once it is received and authenticated through consensus of network users, or once it is coded and added to the blockchain. The answer may lie in a broad interpretation of the legal rules discussed above. However, it is obvious that these rules do not cleanly embrace the concept of smart contracts.

3.4 Establishing Legal 'Intent' in 'Follow-On' Contracting

Some smart contracts have the capacity to enter parties into subsequent, separate 'follow-on' contracts. That is, where parties have voluntarily entered into a smart contract (the primary contract), that contract can itself enter the parties into an additional contract (the secondary contract). The parties may not even have knowledge of the follow-on contract and so two questions arise: (1) can an *intention to create legal relations* be established in this circumstance, and (2) can a smart contract or related electronic agents or 'bots' autonomously enter parties into legally enforceable follow-on contracts?

As to the first question, it is important to note that legal intent is one of the core requirements of a valid contract under English[40] and Australian[41] law. The assessment is objective: the court does not seek to identify the subjective intentions of the parties but instead asks whether reasonable people would have regarded the agreement in question as intended to be binding. Under US contract law, legal intent is typically established as an aspect of offer and acceptance rather than as a discrete element; the courts objectively ascertain whether a party's offer was a genuine manifestation of their willingness to enter into a formal bargain, and whether the other party's acceptance demonstrated

placing acceptance 'at the time and place of sending': Bell, Boyron and Whittaker, above n 23, p 312. This would imply that the postal acceptance rule also applies to electronic communications in that jurisdiction.

[37] See *Okosa v Hall* 718 A.2d 1223 (App. Div. 1998); *Uniform Commercial Code* (UCC) arts 1-103(b), 1-202, 2-206, 2-606.

[38] See Roger LeRoy Miller and Gaylord A Jentz, *Business Law Today* (Cengage Learning, 2010) p 217, where the authors provide a useful discussion as to rule's position under US common law and the *Uniform Electronic Transactions Act* in that jurisdiction.

[39] Norton Rose Fulbright, 'Can Smart Contracts be Legally Binding Contracts?', R3 and Norton Rose Fulbright White Paper (November 2016), p 22.

[40] *Merritt v Merritt* [1970] 1 WLR 1211.

[41] *Riches v Hogben* [1986] 1 Qd R 315; *Woodward v Johnston* [1992] 2 Qd R 214; *Kovan Engineering (Aust) Pty Ltd v Gold Peg International Pty Ltd* [2006] FCAFC 117 (14 July 2006); *ATCO Controls Pty Ltd v Newtronics Pty Ltd* (2009) VR 411.

understanding and desire that, in giving assent, they concluded a formal bargain.[42] The test under French law is *subjective*; a party will only be bound to a contract if they actually intended to be bound[43] and, as with the US, this is traditionally established by examining the agreement – or 'offer/acceptance' – stage of the parties' interactions.[44] This analysis, however, is often still reliant upon tangible *manifestations* of such subjective intention (whether oral, in writing, or by conduct).[45]

It is certainly questionable whether legal intent can be *presumed* to exist in a follow-on contract merely because it ostensibly existed in the primary contract. The courts may take issue with this and determine that legal intention cannot be assumed to 'carry over' into subsequent, autonomously-generated contracts. The consequence of such a finding is that a potentially large number of follow-on contracts may be struck down for want of enforceability. Under the 'reasonable person' test favoured in England and Australia, and the equivalent objective analysis of the parties' agreement in the United States, it would seem presumptuous to blindly assume that the parties would have acquiesced to any *further* agreements stemming from a smart contract without having first properly considered their nature and effect. Similarly, significant issues of proof would arise under French law where the parties sought to prove that they did or did not intend for follow-on contracts to have legal force and bind them and, therefore, that those contracts lacked the requisite *consentement* (consent).

As to the second question – whether a smart contract or related electronic agents or 'bots' could autonomously enter parties into legally enforceable follow-on contracts – the guiding legal principles are even less harmonious. In England, for example, there is authority implying that automated computer systems are incapable of binding parties through implied agency as they lack the consciousness of a human mind.[46] The position is somewhat different in Australia, where s 15C of the *Electronic Transactions Act 1999* (Cth) provides that a contract formed by (a) the interaction of an automated message system and a natural person or (b) the interaction of automated message systems 'is not invalid, void or unenforceable on the sole ground that no natural person reviewed or intervened in each of the individual actions carried out by the automated message systems or the resulting

[42] See *Restatement (Second) of Contracts* (1981), arts 21, 24; *Lonergan v Scolnick* 129 Cal. App. 2d 179 (1954); *Empro Manufacturing Co. v Ball-Co Manufacturing., Inc* 870 F. 2d 423 (7th Circ. 1989).

[43] See French Civil Code, arts 1110, 1134; Commission on European Contract Law, above n 36, p 146.

[44] The courts seek to identify a consensual *accord de volontés* ('meeting of the minds'). 'There is not, in French law, as such a principle that there must be an "intention to create legal relations"': Anne de Moor, 'Contract and Agreement in English and French Law' (1986) 6 *Oxford Journal of Legal Studies* 275, 278. See also Julie M Philippe, 'French and American Approaches to Contract Formation and Enforceability: A Comparative Perspective' (2005) 12(2) *Tulsa Journal of Comparative and International Law* 357, 372-3.

[45] Bell, Boyron and Whittaker, above n 23, p 311.

[46] *Software Solutions Partners Ltd, R (on the application of) v HM Customs & Excise* [2007] EWHC 971. Some international authorities suggest that the fact the parties themselves programmed the smart contract and, therefore, anticipated its capacity to enter them into follow-on contracts, means they must be taken to accept that they may be bound to those follow-on contracts. See for example *Chwee Kin Keong v Digilandmall.com Pte Ltd* [2005] 2 LRC 28 (Singapore).

contract'. As such, a smart contract or other electronic agent could conceivably enter parties into an enforceable follow-on contract (subject to other legal conditions being satisfied, and to the parties' right to amend errors in electronic communications[47]).

The US authorities addressing this issue are notably discordant. Some courts have decided, for example, that an automated response to a contractual offer did not amount to valid acceptance[48] whereas others have found that a search bot acting autonomously in accepting and violating the terms of a contract was deemed to be acting with the authority of the dispatching party.[49] In *State Farm Mutual Automobile Insurance Company v Bockhorst*, the United States Court of Appeals (10th Circuit) held that an automated reinstatement of an insurance policy, though erroneous, was regarded as an action of the insurer and therefore legally enforceable.[50] The legal status of follow-on contracts stemming from a primary smart contract under US law is therefore patently unclear.

Finally, various provisions of the French Civil Code permit the use of electronic contracts.[51] The provisions relating to agency, however, are silent on the issue of *electronic* agents.[52] As we have seen, the French law with respect to establishing contractual intent prioritises the subjective mindsets of the parties, although 'applying the subjective theory to electronic agents faces the difficulties of attributing a "free will" to electronic agents and how such an electronic agent can be said to have "an inner will"'.[53] That being said, *any person* may enter into a contract unless they have been declared incapable of doing so by law.[54] Until electronic agents are unequivocally deemed to lack legal personality, a 'tacit agency' may be inferred under art 1985 of the French Civil Code as between an electronic agent and a human party, conferring authority on the part of the former to enter into follow-on contracts on behalf of the latter. The question remains untested under French law.

3.5 Certainty of Terms

Contracts must be legally certain in order to be enforceable. Under English law, it is often said that the contract must be sufficiently certain in terms of both inherent clarity and completeness in order to bind.[55] The Australian courts endorse a liberal approach and endeavour to attribute meaning to obscure contract terms, deeming the contract unenforceable only where no such meaning can be

[47] See s 15D of the *Electronic Transactions Act 1999* (Cth).
[48] *Corinthian Pharmaceutical Systems, Inc. v Lederle Laboratories* 724 F. Supp. 605 (S. D. Ind. 1989)..
[49] *Register.com, Inc. v Verio, Inc.* 356 F.3d 393 (2nd Cir. 2004).
[50] 453 F. 2d 533 (1972).
[51] See for example Title III, Chapter VII, Sections 1-4.
[52] See French Civil Code, Title XIII.
[53] Abdulhadi M Alghamdi, *The Law of E-Commerce: E-Contracts, E-Business* (AuthorHouse, 2011) p 132.
[54] French Civil Code, art 1123.
[55] See *G Scammell & Nephew Ltd v H C & J G Ouston* [1941] AC 251.

elucidated.[56] The general common law position in the US is that contracts which are indefinite or vague as to their essential terms are unenforceable.[57] The *Uniform Commercial Code* (US), however, provides that sales contracts are not unenforceable even where 'one or more terms are left open' provided the parties intended to make a contract and there exists a 'reasonably certain basis for giving an appropriate remedy'.[58] The American courts prefer to construe contracts so as to give them meaning and establish validity, rather than strike them down for uncertainty.[59] Questions as to the certainty of contract terms in France have tended to focus upon the price, goods/services or other central subject matter to the agreement.[60] Under French law, a contract must have a 'definite object' (*objet*).[61] Provided the fundamental aspects of the contract are clear, it will typically be enforced.

Smart contracts are computer programs coded to perform certain predetermined functions. The language used to code them is completely unintelligible to anyone untrained in programming, which raises a number of interesting questions with respect to their enforceability.[62] The laws of all jurisdictions considered by this article favour certainty as to all critical terms of a contract, with some tolerance for minor imperfections (curable through liberal construction). But how would the content of smart contracts be treated when the courts come to examine whether they are sufficiently *certain*? During the planning phase, the terms drafted in natural language by the parties must then be coded into programming language in order to generate the actual smart contract comprising the agreement of the parties. Ostensibly, then, the document containing the intelligible natural language terms is merely *prefatory to the actual contract* and therefore not relevant to the question of legal certainty. Judges may struggle to regard programming code within a smart contract as legally 'certain'. Moreover, as explained further on, natural language versions of smart contracts would potentially be restricted under the parol evidence rule concerning reference to materials extrinsic to the smart contract itself.

Other issues with certainty may also arise from the use of smart contracts. For example, the courts frequently encounter considerable difficulty giving meaning to normative standards such as 'reasonableness', 'unconscionability' and the like. It is very unclear how a smart contract could be coded so as to give effect to such terms. To provide a realistic scenario, assume that a smart contract incorporated a duty of 'good faith and fair dealing'. How is a computer to judge whether this provision has been violated? As one commentator notes, '[t]rying to explain this to a group of

[56] *Upper Hunter County District Council v Australian Chilling & Freezing Co Ltd* (1969) 118 CLR 429.

[57] See for example: *Laseter v Pet Dairy Products Co* 246 F.2d 747 (4th Circ. 1957); *Robinson v Wilson, Inc. v Stone* 35 Cal. App. 3d 396 (1973); *Rosenthal v National Produce Co* 573 A.2d 365 (DC App. 1990).

[58] Article 2-204(3).

[59] *American Sugar Refining Co v Newman Grocery Co* 284 F. 835 (5th Circ. 1922).

[60] See French Civil Code, arts 1583 and 1589 in the context of sales contracts.

[61] French Civil Code, arts 1108, 1129. There is, however, some allowance for terms which are identifiable in the future (such as the quantity of goods yet to be purchased). See arts 1126-1133.

[62] As to the potential issues arising from interpretation of the content of smart contracts generally, see below at 3.7.

transistors so that it can be computationally executed is currently science fiction (without the use of an enormous amount of code or computing power)'.[63] Moreover, in many cases traditional contracts contain provisions allowing for the enforcement of rights against a defaulting party. The choice to utilise such provisions is one which is critically informed by human judgment; automatic enforcement may not be the best course of action, but the smart contract would know no different.

3.6 Remedial Issues

By virtue of their nature, smart contracts are also susceptible to a number of problems, each of which give rise to certain remedial issues. Smart contracts are essentially computer programs fashioned as conduits for commercial transactions. They are coded to execute specific instructions using immutable programming language. Once on the blockchain, smart contracts proceed in enforcing themselves. Whilst certain parameters may be amendable, smart contracts operating within a blockchain network fundamentally do not – perhaps cannot – change. Computer code is designed to be finite; once on the blockchain, it can be extremely difficult and potentially impossible to access and amend a smart contract's coding.

On the one hand, this might be seen as a positive because human error in execution is eliminated given that data in a blockchain 'is guaranteed to be valid according to certain predefined rules of the system (e.g., there are no double-spends or invalid signatures)'.[64] On the other hand, smart contracts present the risk of errors which may not be reversible or which require extensive efforts to correct.[65] This may result in significant economic consequences for miners. In April 2016, for example, a coding error in the Ethereum-based online Ponzi scheme known as 'GovernMental' resulted in the sizeable 'jackpot' ether payout becoming stuck in perpetuity.[66] Around the same time, online Ethereum-based gambling service Etherdice suffered a similar fate and inadvertently locked its bankroll.[67] Moreover, given the capacity for computer programs (and their coding) to *spontaneously*

[63] Scott Farrell, Claire Warren, Roslyn Hinchliffe and Johanan Ottensooser, 'How to Use Humans to Make "Smart Contracts" Truly Smart' (*King & Wood Mallesons*, 7 July 2016) < http://www.kwm.com/en/au/knowledge/insights/smart-contracts-open-source-model-dna-digital-analogue-human-20160630>.

[64] Delmolino, Arnett, Kosba, Miller and Shi, above n 3, p 3.

[65] Luu, Chu, Olickel, Saxena and Hobor note: 'There is no way to patch a buggy smart contract, regardless of its popularity or how much money it has, without reversing the blockchain (a formidable task). Therefore, reasoning about the correctness of smart contracts before deployment is critical, as is designing a safe smart contract system'. Loi Luu, Duc-Hiep Chu, Hrishi Olickel, Prateek Saxena and Aquinas Hobor, 'Making Smart Contracts Smarter', Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (24-28 October 2016), Vienna, p 254 at p 255.

[66] See https://www.reddit.com/r/ethereum/comments/4ghzhv/governmentals_1100_eth_jackpot_payout_is_stuck/. At the time of writing, the GovernMental website was inactive and offering error prompts: http://governmental.github.io/GovernMental/.

[67] See https://etherdice.io/#game.

corrupt, in which case neither party is necessarily 'responsible', there is potential for disputes as to liability to arise if the risk of technical error eventuates.

Smart contracts therefore give rise to a number of significant remedial issues. These contracts are relatively impervious being designed to be 'permanent' in nature and to integrate smoothly into what is likely to be a voluminous ledger of transactions on the blockchain. As mentioned earlier, errors requiring correction may not be reversible, or at the least would likely require extensive efforts to correct.[68] Whereas error correction with traditional non-digital contracts is relatively straightforward, the same cannot be said of smart contracts. This may present something of a logistical nightmare for courts trying to apply traditional contract law principle to rectify errors with a smart contract.

A related and highly significant remedial issue relates to injunctive relief. Assume, for example, that a party sought to restrain the other party from enforcing (or violating) a term of a smart contract. Depending on the urgency or significance of the situation, one response would be to apply for an injunction from the courts preventing the other party from enforcing or violating the term in dispute. The issue here is that the smart contract is autonomous and self-executing. Unlike a non-digital contract, a smart contract is not capable of simply being 'stopped' instantaneously upon notification to the affected party that it must cease whatever activity is being prohibited by the injunction. Again, it can be seen that enforcing a judicial order which affects contractual relations may well be far more complex in the case of smart contracts.

3.7 Interpreting Content

It is the natural role of the courts to resolve legal disputes between citizens and/or the state. Given that contracts are in the domain of private law, when contractual disputes arise it is for the courts to determine the rights and obligations of each party. This inherently involves reference to the terms of the contract. In the case of a smart contract, however, the terms are – as discussed earlier at 3.5 – encapsulated in computer code that will almost certainly be completely unintelligible to the average lawyer or judge. Reference to the terms in legible linguistic form (in extrinsic materials such as original terms of reference or heads of agreement, negotiation notes, emails etc.) would also seemingly be barred by the parol evidence rule, which prohibits reference to such materials where the express terms have been reduced to a final written agreement.[69] An exception here might be that the

[68] Reversing the blockchain is the first step in remedying any defects with a particular contract within it, regardless of that contract's value or popularity. This is, needless to say, an enormously difficult task: Luu, Chu, Olickel, Saxena and Hobor, above n 65, 255.

[69] See in England/Australia: *Goss v Nugent* (1833) 110 ER 713; *Mercantile Bank of Sydney v Taylor* (1891) 12 LR (NSW) 252. In the US: *Restatement (Second) of Contracts* (1981) art 213; *Uniform Commercial Code* (UCC) art 2-202. A version of the parol evidence rule in the contractual context can be found in art 1341 of the

terms of the smart contract are entirely ambiguous and incomprehensible without reference to such extrinsic materials, in which case the courts may permit resort to them.[70] Expert evidence may also be required, such as qualified programmers equipped to decipher the smart contract code. In any event, the process of construction is very likely to be slowed as a consequence of the need to consider both the contract terms as coded into the smart contract (program) and the original, natural contract terms as drafted by the parties and/or their lawyers.

Smart contracts present other difficulties relating to the expression of their content. As mentioned earlier (at 3.5), it would be highly problematic, for example, for a smart contract to give effect to normative concepts such as 'reasonableness', which are often found in discretionary clauses. How is a smart contract to quantify such a thing as reasonableness by application of a linear algorithmic approach? Another problem would arise where the contract contained a mechanism for variation, which is a common feature in many commercial agreements. It may also be difficult, perhaps near impossible, to reduce particular scenarios articulated in contract terms to computer code. These clauses could not readily be enforced owing to the immutable nature of the blockchain, and the need for professionals versed in programming (which would likely exclude the parties and their lawyer(s)) to do the work.

One final example of an issue which may affect the interpretation of the content of a smart contract is where the contract is dependent upon external sources of information to inform its operation. Assume, for example, that a smart contract of insurance is created to indemnify a homeowner against inclement weather. The contract might be programmed to obtain information relating to rainfall, temperature or other factors from a meteorological agency's website in order to determine if the policy is activated. Alternatively, a smart contract for the sale of shares might be programmed to sell once the shares reach a certain predetermined price. The contract could link to an official stock exchange website in order to determine if the price has been reached, triggering the sale clause. If, however, the external sources in either scenario malfunction or become inactive at any stage, the substantive content of the smart contract could be affected; the contract could potentially commit errors or even fail altogether.

Again, the law must respond but the question here is *how* it would do so. Whereas wrongful or non-performance in a traditional contract can be remedied in a number of ways from self-help to legal action, ensuring the fulfilment a smart contract is, as we have seen, not as simple. The doctrine of frustration (discussed earlier at 3.2) might provide a solution once more although we arrive at the

French Civil Code, though other provisions do affect the manner by which proof may be levelled against parties involved in trade.

[70] This is an established exception under Australian and English law. See for example: *Reardon Smith Line Ltd v Yngvar Hansen-Tangen and Sanko SS & Co Ltd* [1976] 1 WLR 989; *Codelfa Construction Pty Ltd v State Railway Authority of New South Wales* (1982) 149 CLR 337.

same unsatisfactory conclusion of the contract being vitiated entirely. The doctrine may also be inapplicable given that the risk of technical error might be assumed to have been foreseeable and therefore impliedly assumed by the parties. Carter, outlining the position under English and Australian law, explains:[71]

> [I]t is usually said that the event relied upon as frustrating the contract must not have been foreseen by the parties. … If the event was foreseen, and the contract contains no provision covering the event, the inference will usually be drawn that the parties agreed to bear the risk of the occurrence of the event.

As Carter notes, however, the authorities confirm that mere foresight of the possibility of the *cause* of a frustrating event occurring is not sufficient – the parties must instead be found to have foreseen the occurrence of the event in question as a 'serious possibility'.[72] This imposes a slightly higher threshold though it is still arguable, given the infancy of blockchain technology and the various vulnerabilities of smart contracts, that the content of such a contract being affected by programming errors is well within contemplation in the majority of cases. The law thus fails to adapt comfortably to smart contracts, particularly in comparison to traditional non-digital contracts.

4. Other Issues with Smart Contracts

4.1 Security Concerns

All digital technologies are vulnerable to attack from cybercriminals. Cybercrime costs economies around the world billions of dollars each year.[73] As more and more commercial transactions occur via or with the inclusion of digital technologies, and unfathomable amounts of personal and financial information are digitised, the risk of security breaches will continue to increase exponentially. Utilising smart contracts necessarily involves digitising the entirety of the transaction between the parties, which arguably exposes them to greater risk of sensitive information being compromised. In 2016, bitcoin exchange platform Bitfinex and cryptocurrency crowdfunding vehicle The DAO were both hacked and funds were manipulated and stolen.[74]

[71] J W Carter, *Contract Law in Australia* (LexisNexis, 6th ed, 2013) pp 774-5.

[72] Ibid p 775. The author cites *Simmons Ltd v Hay* (1964) 81 WN (Pt 1) (NSW) 358 in support of this proposition.

[73] A recent Forbes article predicted global cybercrime to cost $2.1 trillion by 2019: Steve Morgan, 'Cyber Crime Costs Projected to Reach $2 Trillion by 2019' (*Forbes,* 17 January 2016) <*http*://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#4c1bba3bb0cc>.

[74] Capgemini Consulting, 'Smart Contracts in Financial Services: Getting from Hype to Reality' (2016) p 14.

That being said, smart contracts operate on a blockchain, which is generally either a shared public ledger or a private permissioned ledger. This in itself can offer some form of security, as 'distributed ledgers are not vulnerable to a single point of failure. To be successful, a cyber-attack would need to not only infiltrate one user; it would have to attack multiple copies of the record held across the network'.[75] Regardless, the skill and adaptability demonstrated by many contemporary 'hackers' make it likely that a young and relatively untested technology such as blockchain – one which many major global stakeholders are now looking to actively invest in – will be targeted.

Interestingly, there have even been reports of smart contracts being used for criminal purposes, again calling into question their dependability.[76] The rising value of cybercurrencies and the growing use of smart contracts and blockchain technology have inspired cybercriminals to steal and launder money, demand ransoms, and undertake illicit transactions (one of the more famous being the Silk Road online marketplace saga where the site's owner was charged and convicted of numerous crimes including computer hacking and narcotics trafficking).[77] As experimentation with blockchain continues, and commercial parties opt to engage in transactions through smart contracts, the risk of attack from unscrupulous and innovative hackers increases.

4.2 Scalability

Earlier in the article (at 3.6) two case examples of malfunctioning and incorrectly coded smart contracts – GovernMental and Etherdice – were discussed. These case examples not only highlight the potential harm of erroneous coding, but also demonstrate potential issues with *scalability*. In each case, the coding error centred on miscalculation of the 'gas'[78] required to perform certain functions in each program. The computational power and resources necessary to undertake the respective transactions was grossly underestimated; an error which is perhaps less likely to occur in traditional simple contracts where most risks are well-known and allocated effectively through the terms of the agreement. There is a legitimate risk that current computer infrastructure may not be able to keep pace with the growth of blockchain.

[75] Allens, 'Blockchain Reaction: Understanding the Opportunities and Navigating the Legal Frameworks of Distributed Ledger Technology and Blockchain' (2016) p 4.

[76] See for example Ari Juels, Ahmed Kosba and Elaine Shi, 'The Ring of Gyges: Using Smart Contracts for Crime', *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (24-28 October 2016) Vienna, Austria, 283.

[77] For a concise discussion of Silk Road and the issues associated with its use see James Martin, 'Lost on the Silk Road: Online Drug Distribution and the "Cryptomarket"' (2014) 14(3) *Criminology & Criminal Justice* 351.

[78] Simply put, the term 'gas' describes the internal pricing mechanism for processing a transaction in a smart contract. The party initiating each transaction pays for this process in gas; the miner then collects this payment and adds the transaction to the blockchain. It essentially describes a party's capacity to process a transaction and therefore operates as a fee payable. Thus, a party's gas depletes over time and they must eventually purchase more.

4.3 Workforce Impact

The very premise of smart contracting is disintermediated automation; the contract between the parties executes itself and no trusted intermediary facilitates the exchange of consideration. The intermediary in the vast majority of non-digital commercial transactions is a financial or legal person or authority. The traditional functions of many financial professionals and commercial lawyers may now conceivably be performed by smart contracts, endangering their typically lucrative roles. Indeed, some believe that the financial and legal workforces may suffer losses as 'trustless' blockchain technology cuts them out of the market.[79] It is submitted that smart contracts do not pose quite so serious and immediate a threat as has been suggested. There will still be a place in the world for lawyers and other professionals who are deeply rooted in our global economies and who think in ways that computers simply cannot. As two commentators have noted, artificial intelligence cannot substitute for the organic intuition and perceptive depth of the human mind:[80]

> While many contracts may be automated, in any slightly complex interaction there will be a need for judgement which is still best done by humans. Smart contracts are good at dealing with clear and defined outcomes, but in many ways they are dumb – they can only do exactly what they are programmed to, and they cannot deal with ambiguity …. Really smart contracts still require smart lawyers.

Lawyers are still useful, if not required (particularly in the case of complex transactions), to draft the content which is ultimately translated into computer code. Indeed, they and other intermediaries in the legal, financial and other business sectors would be smart to familiarise themselves with blockchain technology so as to expand their skillsets and capitalise on predicted market demand.[81] There is no question that smart contracts will challenge traditional intermediaries and perhaps assume *some* of their functions, but they will not spell their end. One way to maintain relevance and improve market

[79] See for example: James Eyers, 'Blockchain "Smart Contracts" To Disrupt Lawyers' (*Financial Review*, 30 May 2016) <//www.afr.com/technology/blockchain-smart-contracts-to-disrupt-lawyers-20160529-gp6f5e>; James Eyers and Misa Han, 'Lawyers Prepare for "Driverless M&A" as Smart Contract Era Dawns' (*Financial Review*, 19 June 2016) <http://www.afr.com/technology/lawyers-prepare-for-driverless-ma-as-ssmart-contract-era-dawns-20160616-gpknyz>.

[80] Simun Soljo and David Rountree, 'Unravelled: Blockchain and Why Smart Contracts Still Need Smart Lawyers' (*Allens*, 6 July 2016) < https://www.allens.com.au/pubs/fsr/160706-unravelled-03.htm>. These sentiments are reflected in the full Allens report: 'Blockchain Reaction: Understanding the Opportunities and Navigating the Legal Frameworks of Distributed Ledger Technology and Blockchain' (2016). The report is available at https://www.allens.com.au/data/blockchain/index.htm.

[81] See for example: Marianna Papadakis, 'Blockchain's Big Opportunity for Lawyers' (*Financial Review*, 2 June 2016) <http://www.afr.com/business/legal/blockchains-big-opportunity-for-lawyers-20160531-gp82p2>.

appeal is to embrace the power of smart contracts and blockchain technology and train in the art of coding. As Wang (speaking in the context of lawyers) notes:[82]

> As smart contracts are increasingly used, lawyers may need to gain a basic proficiency in coding to allow them to check that clauses and contractual mechanisms have been appropriately translated to the relevant programming language. This could be met by training as part of continuing professional development obligations or the legal industry could partner with blockchain stakeholders to produce guides and programmable standard smart contracts that could be tailored to a client's needs.

This notion has some notable disadvantages. Having to train legal professionals in coding is a time-consuming process which will itself attract costs and consume a firm's resources. Moreover, little attention has been paid to the fact that blockchain technology may not be readily accepted by *all* factions of commerce and wider society. A smart contract can only be used if the parties – and indeed interested third parties to the transaction – are both willing and able to execute their agreement on a blockchain and do away with traditional trusted intermediaries. These intermediaries are deeply embedded in the modern commercial marketplace so it will take an enormous cultural and technological shift to accept smart contracts as orthodoxy. Smart contracts may thus disrupt commercial activity and cause disharmony in the manners in which commercial parties conduct business, whilst also chipping away at the roles of intermediaries.

5. Conclusion

There are legitimate reasons for people in the legal, commercial, technology and other sectors to be both optimistic and pessimistic about the growing presence of smart contracts. The reasons for optimism are abundant. As this article has discussed, smart contracts have the potential to increase commercial efficiency, reduce transaction and legal costs, and facilitate transparent and anonymous transacting. There are, however, questions surrounding the legal enforceability of smart contracts; it is uncertain whether they will easily adapt to current legal frameworks regulating 'conventional' contracts across jurisdictions. This is something they ultimately *must* do, as Omohundro (envisaging a number of futuristic applications) states: 'self-driving cars [will] need to follow the rules of the road, autonomous business creation [will need] to follow securities laws, and autonomous markets [will] need to levy taxes appropriate for transactions' jurisdictions'.[83] As time progresses, and smart contracts become more widely used and applied in a greater variety of commercial contexts, it is essential that the law keeps pace; uncertainty is the breeding ground for disputation. At present, businesses would certainly be wise to 'factor issues concerning the legal status of smart contracts into

[82] Wang, above n 9, 250.

[83] Omohundro, above n 2, 20.

the wider business case for their deployment'.[84] It is not yet entirely clear whether smart contracts are a smart idea, but there is little doubt the question will soon be tested in the courts.

[84] Norton Rose Fulbright, above n 39, 21.

Author Details

Dr Mark Giancaspro
Lecturer
Law School
The University of Adelaide
North Terrace
ADELAIDE SA 5005

Telephone:	+61 8 8313 0879
Email:	mark.giancaspro@adelaide.edu.au
Website:	http://www.adelaide.edu.au/directory/mark.giancaspro