

# CHAPTER - 9

## "SMART" CONTRACT ON THE BLOCKCHAIN - A BRAVE NEW WORLD FOR UNCITRAL

*Jerry I-H Hsiao\**

### ***I INTRODUCTION***

Commerce generally operates on a centralized model where counterparties transact with each other by means of trusted intermediaries such as:<sup>1</sup> (i) financial institutions that serve as a conduit for parties financial transactions, (ii) retailers that purchase goods from manufacturers and sell them to consumers, and (iii) websites/mobile apps that facilitate the purchase of goods or engagement of services to be provided by third parties. The centralized model creates dependence on the intermediaries and adds costs to each transaction to compensate them for their involvement. In theory, smart contract, helps to reduce reliance on centralized systems and avoid the cost of using intermediaries.<sup>2</sup> Many believe that smart contract is the future of contract. In light of this technological development, the United Nations Commission on International Trade Law (UNCITRAL) has responded to this new challenge, in the era when traditional paper contracts are gradually been replaced by digital or smart contracts. In order to understand the challenge UNCITRAL is currently facing, one needs to understand the background of this new technology.

#### ***1.1 Trustless Public Ledger (TPL)***

Cryptography is a technique for managing secrecy, current uses of cryptography is the development of trustless transfer over network systems. TPL technology liberates individuals from the centralized institutions that moderate online

---

\* Assistant Professor, Faculty of Law, University of Macau.

1 Oliver Herzfeld "Smart Contracts May Create Significant Innovation Disruption" (*Forbes*, 22 February 2016) <[www.forbes.com/sites/oliverherzfeld/2016/02/22/smart-contracts-may-create-significant-innovative-disruption/#33451b062702](http://www.forbes.com/sites/oliverherzfeld/2016/02/22/smart-contracts-may-create-significant-innovative-disruption/#33451b062702)>.

2 Ibid.

transactions by creating a public cryptographically protected transaction list that does not rely on trust in a specific entity to curate the list.<sup>3</sup> TPL, in simple terms is a public list describing the chain of ownership of a given piece of property or something of value.<sup>4</sup> TPL technology removes the middle man, and enables users to exchange digital property securely and anonymously over the network without any prior relationship.<sup>5</sup>

## 1.2 *Smart Contract*

Smart contracts are "computer programs" that can automatically execute the terms of a contract."<sup>6</sup> According to Nick Szabo, smart contracts are "a set of promises, including protocols within which the parties perform other promises. The protocols are usually implemented with programs on a computer network, or in other forms of digital electronics, thus these contracts are "smarter" than the paper-based ancestors. No use of artificial intelligence is implied." These programs address the issue of enforcement and accountability in a trustless system that operates outside the purview of the state. By removing the need for direct human involvement once a smart contract has been deployed onto a distributed ledger, the computer program could make contractual relationships more efficient and economical with potentially fewer opportunities for error, misunderstanding, delay or dispute.<sup>7</sup> In short, the appeal of smart contract lies in (1) the digitization of trust through certainty of execution, and (2) the creation of efficiency through removal of intermediaries and the costs they bring to the transactions.<sup>8</sup>

The basic characteristics of a smart contract are: First, smart contracts are drafted using source code use on computers, they can be standardized and executed at nearly no cost and hence decrease the marginal cost of contracting. Second, for a party valuing certainty, there will be no room for ambiguity of contract interpretation but

---

3 Joshua Fairfield "BitProperty" (2015) 88 S Cal Rev 805, 811.

4 Edward D Baker "Trustless Property System and Anarchy: How Trustless Transfer Technology Will Shape the Future of Property Exchange" (2015) 45 Southwestern L Rev 357.

5 Rob Wile "Satoshi's Revolution: How the Creator of Bitcoin May Have Stumbled onto Something Much Bigger" (*Bus Insider*, 22 April 2014) <[www.businessinsider.com/the-future-of-the-blockchain-2014-4](http://www.businessinsider.com/the-future-of-the-blockchain-2014-4)>.

6 Jay Cassano "What Are Smart Contract? Bitcoin's Killer App" (*Fast Company*, 17 September 2014) <<http://fastcolabs.com/3035723/app-economy/smart-contracts-could-be-cryptocurrencys-killer-app>>.

7 Institute of International Finance "Getting Smart: Contracts on the Blockchain" (11 May 2016) <[www.iif.com/publication/research-note/getting-smart-contracts-blockchain](http://www.iif.com/publication/research-note/getting-smart-contracts-blockchain)>.

8 Cheng Lim and T J Shaw "Smart Contracts: Bridging the Gap between Expectation and Reality" (*Oxford Law Faculty Business Law Blog*, 11 July 2016) <[www.law.ox.ac.uk/business-law-blog/blog/2016/07/smart-contracts-bridging-gap-between-expectation-and-reality](http://www.law.ox.ac.uk/business-law-blog/blog/2016/07/smart-contracts-bridging-gap-between-expectation-and-reality)>.

to execute the contract. So once the contracting parties have agreed to be bound by a particular clause, the smart contract's code immutably binds them to that clause without the possibility of breach. Third, smart contracts are designed on a decentralized format. These characteristics will be further discussed *infra*.<sup>9</sup>

### 1.3 *Blockchain*

Despite the promises, there remain obstacles for smart contract in real life transactions. First, how would a smart contract actually control real assets so that it could enforce an agreement? And second, what computer would be trusted to "execute" those terms in a way that both parties could rely upon?<sup>10</sup> The TPL protocol aggregates each transaction into a public ledger called the "blockchain", a public list and ledger of every Bitcoin transaction.<sup>11</sup> The blockchain is nothing more than a transaction log, and each transaction log is authenticated and verified by a series of mathematical proofs which make it near impossible to either double spend or to intercept or reroute payments in the middle of a transaction.<sup>12</sup>

Blockchain technology represents the next step in the peer-to-peer economy. By combining peer-to-peer networks, cryptographic algorithms, distributed data storage, and a decentralized consensus mechanism, it provides a way for people to agree on a particular state of affairs and record that agreement in a secure and verifiable manner. Blockchain is encrypted and organized into smaller databases referred to as "blocks". Every block contains information about a certain number of transactions, a reference to the preceding block in the blockchain, as well as an answer to a complex mathematical puzzle, which is used to validate the data associated with that block. Since, blockchain is always kept in synchronization, there is only ever one true record of ownership - essential to prevent anyone trying to double spend their assets by sending it multiple parties at the same time. Because it is impossible to edit a blockchain once it has been properly updated, parties have mathematically-enforced confidence that the record of their ownership will persist into the future.<sup>13</sup>

---

9 Joshua Fairfield "Smart Contracts, Bitcoin Bots and Consumer Protection" (2014) 71 Wash & Lee L Rev Online 35, 39.

10 Josh Stark "How Close Are Smart Contracts to Impacting Real-World Law?" (*Coindesk*, 11 April 2016) <[www.coindesk.com/blockchain-smarts-contracts-real-world-law/](http://www.coindesk.com/blockchain-smarts-contracts-real-world-law/)>.

11 Nikolei M Kaplanov "Nerdy Money: Bitcoin, the Private Digital Currency, and the Case against its Regulation" (2012) 25 Loy Consumer L Rev 111, 118.

12 Satoshi Nakamoto "Bitcoin: Peer-to-Peer Electronic Cash System" <<https://bitcoin.org/bitcoin.pdf>>.

13 Stark (above n 10).

## II WHY SMART CONTRACTS?

With all the hype surrounding smart contracts, there are three issues that need to be assessed in order to see whether smart contract brings a paradigm shift to contract law. The first is the difference between smart contract and traditional contract; second, what is the difference between *ex ante* and *ex post* contract enforcement and third, whether contract law that is based on *ex post* amenable to *ex ante* smart contracts.<sup>14</sup>

### 2.1 Current Application of Smart Contract

Prior to the 2008 financial crisis, exchanges involving securities regularly took up to half a week, while loan settlement could extend to 20 days or more. This time lag has increased counterparty risk with serious regulatory consequences. Smart contract is able to shorten settlement time from days or weeks to minutes, thus mitigating risk and freeing up capital in the process.<sup>15</sup> Many companies are now experimenting with smart contract, for example, Japan's Bank of Tokyo-Mitsubishi UFJ is now digitizing contract signing on blockchain for the bank's internal work orders and by 2018 the bank aims to use smart contracts in transaction between the bank and IBM.<sup>16</sup> While in the meantime, lawyers in Australia's King & Wood Mallesons are learning how to code smart contracts.<sup>17</sup>

New York-based Symbiont, has created proprietary smart securities technology that allows financial instruments such as corporate bonds, syndicated loans, and bilateral swaps to be a model in an easy to understand programming language. In the public sector, the state of Delaware, where over half of the public trade companies in the United States are incorporated, is starting to allow using smart contract technology to register companies, track share movements and manage shareholder communications in an automated digital environment.<sup>18</sup>

### 2.2 The Differences between Traditional Contract and Smart Contract

Smart contract is basically a "data-oriented" contract and is one in which the parties have expressed one or more terms or conditions of their agreement in a

14 Harry Surden "Computable Contracts" (2012) 46 UC Davis L Rev 629, 632.

15 Institute of International Finance (above n 7).

16 Mayuko Tani "Tokyo-Mistubishi UFJ Starts Blockchain Trial in Asia" (*Nikkei Asian Review*, 21 September 2016) <<http://asia.nikkei.com/Business/Companies/Tokyo-Mitsubishi-UFJ-starts-blockchain-trial-in-Asia>>.

17 James Eyers "Blockchain 'Smart Contract' to Disrupt Lawyers" (*AFR.com*, 30 May 2016) <[www.afr.com/technology/blockchain-smart-contracts-to-disrupt-lawyers-20160529-gp6f5e](http://www.afr.com/technology/blockchain-smart-contracts-to-disrupt-lawyers-20160529-gp6f5e)>.

18 Institute of International Finance (above n 7).

manner designed to be processable by a computer system. In other words, instead of using natural language, smart contracts use data to facilitate computer analysis, automation, or communication of the contractual obligations. This is indeed the first difference between traditional contract and smart contract, the form in which they are expressed. However, to say that a contract is "data oriented" is not to suggest that every aspect of an arrangement has been represented in computer processable form.<sup>19</sup> As in smart contracts, the data-oriented label simply suggests that the parties have decided that some subset of key terms would benefit from being represented as computer processable data.<sup>20</sup>

The second difference concerns the interpretative audiences. Traditional contracts are intended to be read by people but for smart contracts, they have the additional party that is the computer systems. The third difference is the smart contracts differ in the way which they acquire substantive meaning. In a traditional contract, the meaning arises from the shared understanding of language used by the parties but in smart contract, the parties employ explicit process to endow data with substantive meaning.<sup>21</sup> Therefore, smart contracts are automated when they are programmed with code able to: 1) understand what has been promised under what conditions; and 2) compare what has been promised contractually to what has (or has not) happened.

### ***2.3 Ex Ante and Ex Post Contract Compliance***

By specifying in computer processable form the core terms of a contract, the meaning of these terms, and data relevant to assessing conformance with those terms, contracting parties can sometimes enable automated, prima facie determinations as to compliance.<sup>22</sup> Automation is made possible in smart contracts if some contract terms or conditions have been capable of translation into a consonant set of computer instructions and if the existing data relevant to compliance with contract terms was available in computer-processable form that the parties could provide to the computer for automated comparisons.<sup>23</sup> Using computers, the parties are using an *ex ante* method to guarantee contractual compliance, and explicitly forbearing in accepting the occasional incorrect automated assessment for the sake of efficiency and certainty.<sup>24</sup>

---

19 Surden (above n 14) 640.

20 Ibid.

21 Ibid.

22 Ibid 658.

23 Ibid 664.

24 Ibid 680.

By using smart contracts, the parties are actually changing the paradigm of contract practice from *ex post* authoritative judgment to *ex ante* automated assessments. Parties are into smart contract because they believe that the *ex ante* automated results will only infrequently diverge from an authoritative decision-maker such as a judge. In this way, the parties deliberately forbear from *ex post* corrections for the sake of *ex ante* efficiency. Hence, parties to smart contract could architect their contractual framework so as to increase the legal certainty of their smart contract by agreeing up-front, to be held to these automated conclusions.

### **III THE LIMITS OF SMART CONTRACT**

The hype surrounding smart contract pushes commentators to say that it is going to disrupt a wide variety of technologies, even the profession. However, there remain doubts regarding the use of smart contract. For example, some commentators questioned the utility of smart contract, and state that smart contract will normally be used on low value and/or simple transactions, such as the sale and purchase of a car.<sup>25</sup> Even in the case of simple purchase and sale contracts, only certain parts of agreements will be translated into smart contracts, such as clauses dealing with the payment of funds and transfer of titles to shares. However, other actions, such as monitoring warranty breaches, may continue to be done manually.<sup>26</sup> In addition, since parties to contract can pay coders to tailor smart contract to suit their specific needs, although it gives the negotiation power back to customers in on-line transactions,<sup>27</sup> it nonetheless also adds more transaction costs than traditional standardized contracts. There are also cases in which an attack on the Distributed Autonomous Organization (DAO), a collection of smart contracts, drained \$53 million by a participant who found and exploited a weakness in the code before changes were made to the computer code to restore the funds.

#### **3.1 The Link to the Physical World**

These doubts were raised because commercial exchanges are often very complex. Smart contract can prove to be very inflexible, unable to adjust to changing circumstances and the parties' references. Sometimes, circumstances might change in a way not foreseen by the parties at the time when they entered into the contract, or the parties might have foreseen the problem but deliberately refrained from raising

---

25 Andy Robinson and Tom Hingley "Smart Contracts: The Next Frontier?" (*Oxford Law Faculty Business Law Blog*, 23 May 2016) <[www.law.ox.ac.uk/business-law-blog/blog/2016/05/smart-contracts-next-frontier](http://www.law.ox.ac.uk/business-law-blog/blog/2016/05/smart-contracts-next-frontier)>.

26 *Ibid.*

27 Fairfield (above n 9) 39.

it during the negotiations for fear that they might fail.<sup>28</sup> The parties might also be in a situation where they do not want the contract to be executed strictly. Hence, drafting of contract using natural language allows this level of ambiguity.

For example, setting up a blockchain based land register on a server or coding smart contract to be recorded as a transaction on a blockchain application may prove to be the easy part.<sup>29</sup> Verifying that a person claiming that he has title to a piece of land or verifying that the holder of a public key is who he claims to be, will often be an impossible task.<sup>30</sup> In general, all rights and obligations registered on blockchain applications must rely on the validity under applicable law, and often on the certification by some government or third party authority, and establishing the physical links is often the most cumbersome and expensive part to be overcome.<sup>31</sup>

### 3.2 *Smart Contract as Complete Contract?*

If smart contracts are immutable, unstoppable, and irrefutable computer code, the code implicitly or explicitly declares what will happen in every possible event during the life of the contract.<sup>32</sup> However, traditionally most contracts are incomplete in the sense they do not specify what will happen in every future situation but rather leave that to be determined later. There are reasons why incomplete contracts are so common; the most obvious reason is that it is often too costly to anticipate and agree to unambiguous contractual terms for every set of situations. Incomplete contracts also make renegotiation less costly or more efficient.

Smart contracts are theorized to be complete contracts by focusing on *ex ante* rather than *ex post*. However, the DAO case was incomplete as it failed to anticipate the possibility that coding errors could result in unexpected wealth transfers. In addition, smart contract may deal with commercial scenarios so complex and unpredictable that the code will fail to embed all possible answers to all possible questions.<sup>33</sup> Contract also has other issues such as duress, fraud, forgery, lack of legal capacity and unconscionability. Traditionally, the court provides remedies to injured parties if those scenarios should occur. For a smart contract that aims to avoid the

---

28 E Allen Farnsworth "Meaning in the Law of Contracts" (1967) 76 Yale LJ 939, 956.

29 Martin von Haller Gronbaek "Blockchain 2.0, Smart Contracts and Challenges" (*Bird & Bird*, 16 June 2016) <[www.twobirds.com/en/news/articles/2016/uk/blockchain-2-0--smart-contracts-and-challenges](http://www.twobirds.com/en/news/articles/2016/uk/blockchain-2-0--smart-contracts-and-challenges)>

30 Ibid.

31 Ibid.

32 Larry D Wall "'Smart Contracts' in a Complex World" (*Federal Reserve Bank of Atlanta*, July 2016) <[www.frbatlanta.org/cenfis/publications/notesfromthevault/1607](http://www.frbatlanta.org/cenfis/publications/notesfromthevault/1607)>.

33 Gronbaek (above n 29).

third party intermediary such as the courts, is likely to have serious consequences. For smart contract to replace traditional contract, it needs to show that the expected benefit to the contracting parties exceeds the expected costs of not solving all the problems.

### 3.3 *Contract Law and Smart Contract*

Since smart contract is a computer programme, it raises certain issues where contractual obligations are complex. For example:<sup>34</sup> First, parties may negotiate terms that are not capable of being assessed deterministically by a computer program; Second, parties may import indeterministic concepts of reasonableness or appropriateness that again are not suited for algorithmic determination; Third, the expression of an obligation in code may not accurately reflect the agreement between the parties; and fourth, the contract may itself contain a further agreement to agree, or a mechanism for amending the contract.

The issue regarding smart contract is even more prominent when it wishes to happen independently of the surrounding legal framework. But what if the code base does not reflect the parties understanding of the contract like in the case of mistake?<sup>35</sup> What if the effect of the code base was represented by a different party from he who claimed to be in the situation of misrepresentation? And what if the party does not even have the legal capacity to enter into smart contract in the first place?

As this paper has shown, the code could not take everything necessary into account, like the discussions *supra*, smart contract will be applied in limited cases as it could not ensure compliance *ex ante* in all smart contracts. Although it provides a guarantee of execution to a certain extent, it cannot verify whether the contracting parties have the legal capacity to get into legal relationships or business capacity to make an agreement. It does not care whether there is truly a "meeting of minds" between contractual parties; there is no possibility for the contract to be void or voidable. Of course, one can argue by saying that smart contract will only be agreed upon when conditions have been satisfied, so once satisfied, execution is the logical conclusion. However, although codes are not natural language that might be vague or ambiguous, leaving space for interpretation, do contracting parties actually know what the code means or what they assume the code means? If there are misunderstandings regarding to the contract, can the parties rely on contract law or the court for help?

---

34 Lim and Shaw (above n 8).

35 See eg *Raffles v Wichelhaus* (1864) 2 H & C 906.



## IV WAYS FORWARD?

With the issues at hand, this paper proposes that smart contract has its potential but now it is limited to those terms which are machine-readable, because no AI is involved, the computer could only understand what the programmer wants it to understand. Hence, like the example above, if there are coding errors, smart contract will lose its purpose and show it is inferior to traditional contracts. Smart contract, at the moment, seems to work better with terms involving numbers, contracts that do not need much translation of natural language into codes and generally two party contracts, hence to combine the advantages of both *ex ante* and *ex post* contracts.

### 4.1 UNCITRAL

UNCITRAL, which is a major player in the shaping of regulations for electronic modes of communication in international trade and e-commerce for the past twenty years, has not overlooked this issue. In July 2017, UNCITRAL has accommodated TPL in its explanatory notes in the (MLETR).<sup>36</sup> UNCITRAL's initiative is a good start for the international community because as of date, there are no international legal frameworks for blockchain technologies.<sup>37</sup>

MLETR has tried to address some of the issues raised earlier, for example, MLETR requires a reliable method to be used to identify the person to satisfy the signature requirement.<sup>38</sup> In case a signatory uses a pseudonym, the explanatory notes suggest that factual elements outside the TPL may be relied upon to link pseudonyms to the real names.<sup>39</sup> However, this suggestion relies on an *ex post* mechanism because a list of *ex ante* reliable methods to deter reliance on unreliable methods needs to be reviewed from time to time as neither the configuration of a central registry nor the algorithm of blockchain is permanently fixed.<sup>40</sup> Hence, although MLETR has tried to provide some guidance for smart contract, there are still further issues that need to be addressed.

---

36 UNCITRAL "UNCITRAL Model Law on Electronic Transferable Records" (*United Nations*, 2017) <[www.uncitral.org/pdf/english/texts/electcom/MLETR\\_ebook.pdf](http://www.uncitral.org/pdf/english/texts/electcom/MLETR_ebook.pdf)>.

37 Riccardo de Caria "A Digital Revolution in International Trade? The International Legal Framework for Blockchain Technologies, Virtual Currencies and Smart Contracts: Challenges and Opportunities" (*UNCITRAL*, 9 June 2016) <[www.uncitral.org/pdf/english/congress/Papers\\_for\\_Programme/5-DE\\_CARIA-A\\_Digital\\_Revolution\\_in\\_International\\_Trade.pdf](http://www.uncitral.org/pdf/english/congress/Papers_for_Programme/5-DE_CARIA-A_Digital_Revolution_in_International_Trade.pdf)>.

38 Article 9 "Where the law requires or permits a signature of a person, that requirement is met by an electronic transferable record if a reliable method is used to identify that person and to indicate that person's intention in respect of the information contained in the electronic transferable record".

39 UNCITRAL (above n 36) p 30.

40 Aaheree Mukherjee "Smart Contract-Another Feather in UNICTRAL's Cap" (8 February 2018) Cornell Int'l LJ Online <<http://cornellilj.org/smart-contracts-another-feather-in-uncitrals-cap/>>.

## 4.2 *Traditional Contract + Smart Contract*

Another solution is to combine smart contract with traditional contract and let those terms which could be executed via computer be executed as smart contract while the rest remain as traditional contracts. In other words, traditional contract should be the main source of interpretation and smart contract a supplement. In this sense, should disputes arise, parties can always refer to traditional contracts for clarification. Therefore, unless it is a smart contract which can execute perfectly without any future dispute, it is recommended for the time being to subject smart contract together with traditional contract as well as contract law. By combining contract law, traditional contract with smart contract should be the way forward for smart contracts. While society is still experimenting with smart contract, and regulators thinking how to regulate this new technology, it is dangerous to transfer from traditional contract to smart contract without any supplementary measures. In addition, it is also unrealistic to allow smart contracts to get rid of all third party intermediaries.

## V *CONCLUSION*

This paper has tried to explain the concept of smart contract and its current application. Although it has provided much potential and many believe it will disrupt the current practice of commerce. It is still too early to conclude whether this will become true or remain science fiction. This paper points out three issues that need to be further investigated: First, although smart contract has the potential to be more efficient and effective, whether all contractual terms can be translated into codes and executed through mathematics and algorithm remains an issue. Second, smart contract is based on a binary zero-sum logic that does not appear in all real life contract cases. Third, the decentralized concept is also problematic, as it aims to solve all contractual issues *ex ante*. Fourth, although UNCITRAL has been looking into the matter, more sophisticated solutions are still needed. So, will smart contract bring a paradigm shift to contract law? Probably not in the near future, and we will see more traditional contracts and smart contracts coexisting to supplement each other but not to replace the other.