COMPUTER LAW & SECURITY REVIEW ■■ (2017) ■■–■■

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Is a 'smart contract' really a smart idea? Insights from a legal perspective

Mark Giancaspro *

Law School, University of Adelaide, Adelaide, SA, Australia

Keywords:
Smart
Contract
Law
Enforceability
Blockchain
Technology
Computer
Program
Intermediary
Ledger

ABSTRACT

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.

1. Introduction

As early 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 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.

* Law School, The University of Adelaide, North Terrace, Adelaide, SA 5005, Australia.
E-mail address: mark.giancaspro@adelaide.edu.au.
http://www.adelaide.edu.au/directory/mark.giancaspro.

[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.

http://dx.doi.org/10.1016/j.clsr.2017.05.007
0267-3649/

Please cite this article in press as: Mark Giancaspro, Is a 'smart contract' really a smart idea? Insights from a legal perspective, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.05.007

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 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:

```
1  data Alice, Bob
2  data deadline, threshold
3
4  # Not shown: collect equal deposits from Alice and Bob
5  # We assume StockPriceAuthority is a trusted third party contract that can give us the price
   ↪  of the stock
6
7  def determine_outcome():
8    if block.timestamp > deadline:
9      price = StockPriceAuthority.price()
10     if price > threshold:
11       send(Alice, self.balance)
12     else:
13       send(Bob, self.balance)
```

[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.

[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.

Please cite this article in press as: Mark Giancaspro, Is a 'smart contract' really a smart idea? Insights from a legal perspective, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.05.007