

Scientia Nobilitat Reviewed Legal Studies



The Republic of Poland
2014



SCIENTIA NOBILITAT

REVIEWS FOR COUNCIL OF SCIENTIFIC JUDGES

Scientia Nobilitat

Reviewed Legal Studies

Łask, The Republic of Poland 2014

Recenzenci/Reviewers
Opiniodawcy/Advisers:

Doc. PhDr. Dušan Stanek, CSc.
Prof. JUDr. Marián Vrabko, CSc.
doc. JUDr. Markéta Selucká, Ph.D.
JUDr. Vladislav Mičátek, Ph.D.
Mgr Robert Siuciński

Scientia Nobilitat

Platform for Exchange of Scientific Ideas

Aneta Tyc, e-mail: conference@scientianobilitat.eu

ul. Miła 7,

98-100 Łask,

The Republic of Poland

Projekt okładki/Cover design:

Dominik Bielak

Partner/Sponsor:

malito.pl

&

New Engineering Torino S.r.l.

Copyright:

Copyright © Scientia Nobilitat and the Authors, Łask, The Republic of Poland 2014

ISBN 978-83-940589-0-6



SCIENTIA NOBILITAT

PLATFORM FOR EXCHANGE OF SCIENTIFIC IDEAS

Wszelkie prawa zastrzeżone. Nieautoryzowane kopiowanie jest naruszeniem obowiązującego prawa.
All rights reserved. Unauthorized duplication is a violation of applicable laws.

Spis treści/Table of Contents

Samuel Bourque, Sara Fung Ling Tsui	p. 4
A LAWYER'S INTRODUCTION TO SMART CONTRACTS	

Rastislav Munk	p. 24
ANIMAL PROTECTION IN SLOVAK REPUBLIC	

Veronika Munková	p. 31
L'INCOMPATIBILITÀ DEL MANDATO DEL SINDACO CON ALCUNE CARICHE	
INCOMPATIBILITY OF AN OFFICE OF COMMUNITY MAYOR WITH SOME OTHER FUNCTIONS	

Iva Šťavíková Řezníčková	p. 39
UNFAIR CONTRACT TERMS IN THE CZECH REPUBLIC AFTER RECODIFICATION OF PRIVATE LAW	

Jana Šmelková, Kristína Jurkovičová	p. 45
CROSS-BOARDER MERGERS IN THE SLOVAK REPUBLIC FROM THE CORPORATE LAW AND TAX LAW PERSPECTIVE	

Ivan K. Mugabi	p. 52
CONFLICT OF LAWS CROSS TO PUBLIC INTERNATIONAL LAWS: THE CONFLICTING MODELS IN THE CONCEPTUALISATION OF DISABILITY RIGHTS UNDER INTERNATIONAL HUMANITARIAN LAW AND HUMAN RIGHTS LAW	

A LAWYER'S INTRODUCTION TO SMART CONTRACTS

Samuel Bourque
Sara Fung Ling Tsui

Abstract

Smart contracts represent some of the most exciting breakthroughs following Bitcoin and Blockchain-based technologies. However, much of the discussion has been around the technical aspects with the actual legal and practical implications left vague. This discussion bridges the gap between the legal world and the upcoming crypto-economy that will be shaped by Smart Contracts and proposed Decentralized Autonomous Organizations; and composes a cursory examination of the legal implications of Smart Contracts:

- (1) what are Smart Contracts?
- (2) are Smart Contracts considered contracts in law?
- (3) what are practical uses for Smart Contracts?
- (4) can Smart Contracts opt-out of the legal system?
- (5) are DAO/DACs outside of courts' jurisdiction?

Keywords

Smart Contracts, cryptocurrencies, technology, bitcoin, legal policy

1. Smart Contracts

1.1. The Short Answer

Simply put, a Smart Contract (“SC”) is a self-executing contract. To wit, SCs are just like traditional paper contracts drafted in natural human language only that SCs specifically are drafted electronically in a computer interpretable language. The important effect is that the computer system that interprets the SC can execute some of the terms of the contract.¹

The nearest analogy for a SC in the traditional view is that of an executor (in the older sense—not its probate definition); or in a more modern sense, an administrator or a servicer of a contract.

An appropriate analogy for the reader to envision would be that of two masters that share a servant; the latter has the ability to read and is bound to obey both his masters’ signed instructions. When the two masters draft and sign an agreement; the servant, upon receipt of the written contract, would oversee and perform the contractual obligations through to the contract’s termination. To draw the parallel back to SCs, the masters are the parties to the contract and the SC is the servant that executes the contract obligations.

1.2. Pure Smart Contracts vs. Smart Contracts Lite

Not all SCs are created equal—some are “smarter” than others. There are three perpendicular axes to consider:

- (1) the level of automation of the execution of the contract;
- (2) the extent of separation between the actual agreed upon terms and the executed code; and finally

¹ For more information, please visit: <http://szabo.best.vwh.net/contractlanguage.html>; N. Szabo, *A Formal Language for Analyzing Contracts*, 2002.

(3) the custodial rights and/or discretion of the SC and its execution from the parties.

Firstly, let's discuss the level of automation: there long have been many contracts for which its terms in part have been established in computer-executable code. Such examples are: any online merchant,² for which manual interaction is needed—e.g. shipping; conversely, data-only online merchants may be fully automatable as there may be no manual intervention required for the transaction to clear.

Secondly, let's go over the distinction between the actual contract and the SC. Generally in an online vendor scenario, the actual contract is an adhesion contract spelled out by the terms of use and/or terms and conditions on the website's sitemap, or on purchase confirmation display. The code executing the contract is then separate from the actual terms; and hence may be disjoint in a few separate ways—one could presume skewed in the vendor's favor, given the lack of transparency.

This leads to the third issue—regarding the custodian of the code. In keeping with the analogy of an online retailer, the code resides within the merchant's control; furthermore, the customer may never have a chance to review or audit it at any time. Understandably, most online customers may not have the level of sophistication to review—or even want to review—such code. However, with the *status quo*, a customer sophisticated in the ability to understand code and/or with a specialized need would scarcely be given authorization to audit the merchant's code. This is not for nefarious reasons, but due to information security concerns—merchants could/should not open their systems up to outside actors as it not only contains proprietary information but personal information of their other customers, which must be protected by law in most jurisdictions. The alternative scenario is one in which the code is held by a trusted 3rd party. Therefore, no party to the contract has special discretion over the contract. As mentioned previously, the 3rd party custodian ensures a minimum of disjunction between the terms and the code; additionally transparency over the complete set of express terms is ensured.

Pure SCs propose a change in normativity in which the actual code is to be the agreement; therefore, no possibility for disjunction between the execution and the contract.³

1.3. Novelty

As just described, SCs as a concept are not exactly new, and pure SCs do not involve any novel technological breakthroughs. Therefore, one could ask: why are SCs making a surge only now? The reason is that most interesting contracts involve monetary transactions. This was impossible for several reasons:

(1) actual cash is physical and SCs are obviously limited to the virtual world of the Internet; and

(2) digital cash, as bank's cash reserves, is heavily regulated and its use is not allowed in programmatic fashion by individuals.

This is for obvious information security reasons—as in this case, the information is money—and its breach can amount to a financial and economic tragedy. Therefore, drafting SCs to handle regular money, whether cash or digital, is not technically feasible or allowable.

As we will discuss, there already exists some notion of SCs, but they generally did not handle

²There are many online merchants available and some well known ones would be Amazon.com, eBay and the up and rising Alibaba. Please see <http://projects.wsj.com/alibaba/> for more information on Alibaba.

³Assumes no “bugs,” which will be covered infra.

actual assets; rather they rely on issuance and transfer of credit, i.e. debt, upon which does not guarantee performance, and is vulnerable to fraudulent activity.

1.4. What Are Cryptocurrencies?

This is where cryptocurrencies come in. Bitcoin is the first cryptocurrency to gain wide traction as a means of exchange and store of value; this is evidenced by its market capital, which stands at US\$5B⁴ and is potentially poised to gain many multiples if it becomes more widely adopted. Cryptocurrencies are important as they allow unfettered, programmatic access to means of exchange.⁵

1.5. What's New Then?

Now we can identify the true novelty: the advent of combining self-executing contracts and cryptocurrencies. Such a combination allows unforeseeable possibilities, in the same way that the Internet escalated the level of possibilities for commercial applications.

In sum, the novel features of SCs are:

- (1) transparency of the agreement and its execution;
- (2) independence of the agreement's execution and the parties;
- (3) automation of the agreement's obligations.

2. Properties of Smart Contracts

SCs are an aggregate of many components, each of which must be properly understood to grasp their complete legal ramifications. What follows is a distilled description of each with minimal emphasis on their technical details.

2.1. Parties

The first aspect of SCs that we'll examine is that of its parties. Each party must:

- (1) be identifiable; and
- (2) sign—or otherwise indicate acceptance to the agreement and its terms.

This all depends on the concept of identity of the party. In digital commerce, the use of the Private Key Infrastructure⁶ ("PKI") is already well established as means of identification.⁷ In simple terms, it is an equivalent to a certificate of identity that can be verified by the sole holder of a private key—similar to how a PIN verifies a bankcard holder—that must not be shared. So long as the private key is privately held, its owner can be demonstrably verified beyond a reasonable doubt.⁸

The most fundamental concept is that a PKI certificate (also termed public key) and its private key can be used independently to encrypt information so that only its corresponding key can decrypt (unlock) the information into a meaningful form; e.g. a simple message can be

⁴As of November 2014; source from Crypto-Currency Market Capitalization, available at: <http://coinmarketcap.com>.

⁵Available at: www.bitcoin.org/en/faq [accessed 18 November 2014].

⁶The PKI patent is publicly viewable at: www.google.com/patents/US8767965. The PKI was invented by Giovanni Di Crescenzo, Tao Zhang and Robert G. White.

⁷Ibid. As explained by the technology of the PKI, one of its functions is of identification when required.

⁸Ibid n 5.

encrypted by the private key and decrypted by its public key, and vice-versa.

Using a combination of such techniques, the SC can:

- (1) be signed,
- (2) make the parties verifiable,
- (3) be encrypted, and
- (4) guarantee the integrity of the code.

This will be detailed further in part 4.

2.2. Capacity

SCs may have their own web presence, either as a webpage or an accessible web service. Since they are identifiable PKI-wise, they may also be equipped with their own cryptocurrency wallet, or alternatively have custody of digital assets; e.g. electronic title or certificate recognized by an authorized system.

As an aside, there has been a movement towards digitization of assets, presumably to enhance efficiency and minimize paperwork in an attempt to modernize. One notable case is that of the United States that has the Mortgage Electronics Registration System (“MERS”)⁹, where mortgages and property transfers are executable electronically.

2.3. Interpretation

The terms of the SC are to be written in machine-readable code; to wit, this implies that it be written in a language that established CPUs, OSes and compilers/interpreters have the ability to interpret its instructions. Generally, it can be expected that SCs are to be written in standard programming languages, presumably high-level languages that allow for more abstraction, i.e. closer to human language; as opposed to assembly instructions which are very close to low-level machine instructions, or—even-worse—binary code.

Obviously, the language used ought to ultimately be unambiguous, and not dependent on the specific technology on which it is executed.

2.4. Offline Clauses and Contracts

Conversely, not all SCs or their clauses need to be neither interpretable nor executable. This can be useful in many ways, either as means of memorializing the purpose, such as the preamble, of the agreement; or it can be used to indicate the governing law in case there is a dispute. Such examples are: memoranda of understanding, governing law clauses, and so on. Alternatively, whole contracts may not be meant to be enforced. In such a case, the SC system can be used as simple storage and can document the signatures and evidence the time at which the contract was made.

⁹Information taken from: [www.mersinc.org]. Accessed 18 November 2014. MERSCORP Holdings, Inc. owns and operates the MERS System, a national electronic registry system that tracks the changes in servicing rights and beneficial ownership interests in mortgage loans that are registered on the registry. The MERS System is a member-based organization made up of thousands of lenders, servicers, sub-servicers, investors and government institutions. MERS serves as the mortgagee in the land records for loans registered on the MERS System, and is a nominee (or agent) for the owner of the promissory note. The MERS System is a national electronic database that tracks changes in mortgage servicing and beneficial ownership interests in residential mortgage loans.

2.5. Conditionals

Computer programming is fundamentally a large aggregate of simple instructions and conditional statements; i.e. if something is true: then do something; else: do something different. If interpreting the conditional statements, the SC will mostly require outside information. Assuming the SC and its custodian have Internet access, it will be able to query anything accessible on the Internet.

As an example, one can imagine a friendly wager between friends where they bet on the result of a hockey match. The SC could be instructed to—upon conclusion of the match—query the match scores from an authoritative website or web service. Given those results, the SC then determines who wins the bet and awards the winnings accordingly.

This enables the parties to rely on trusted 3rd party sources of information, without relying on one of the parties to produce the crucial data—drastically reducing the risk of conflicts-of-interest.

2.6. Events and State

SCs must keep a record of events in order to interpret and track all obligations, just as a computer program does. Therefore, as various milestones are reached within a contract, such events are to be noted; or as certain values are determined and/or calculations to be made, those may need recording as well for future use.

The full set of such recorded values constitutes the SC's state. Assuming that each event's timestamp is recorded, then in tandem with the code, one ought to be able to reconstruct the history of the SC at any given point.

Furthermore, SCs' code may define instructions to be followed when an event occurred—same as event-driven computer programming. Such events can be triggered:

- (1) by an external prompt, or
- (2) based on a timer or schedule.

The typical purpose for the former type of events is for when instructions are to be followed, or data registered, when a party triggers it. Alternatively for the latter case, its purpose would generally be to indicate some expiration, or that a performance is due.

A simple example that illustrates both cases is one about an online purchase that requires shipment with a 10-days no-questions-asked return policy. Once the buyer and the seller both sign, then the buyer would deposit the cryptocurrency payment into the SC. The seller could manually indicate by triggering an event, which would notify the buyer that the package has been posted, along with its tracking number—the former type of event discussed the previous paragraph. From this point, the SC—if properly drafted—could conceivably track the shipment online to find out its date of arrival; at which point, it would start the 10 day timer at whose alarm would expire the return policy—the latter type of event discussed in the previous paragraph.

This type of functionality is required to track a contract through its various steps.

2.7. Performance

On the opposite end of things, once the SC has interpreted the conditionals and has

determined the instructions to execute, the SC can then perform any action that is possible on the Internet; e.g. posting something online, sending an email, making a Bitcoin payment.

This is the ultimate end, without which SCs would scarcely be useful. Alternatively though, even without any ability to perform the substantial purpose of the contract, it can act as the manager and/or timekeeper of the contract; e.g. notify the party of the due obligation at a schedule time.

2.8. Workflow

Contract Law is a well-entrenched set of rules encompassing all aspects of contracting: from their formation, to their termination. To wit, there is a prescribed series of steps through which parties have to follow.

One such procedure is that of amendment. The process for an SC is obviously different than the process for amending paper contracts, yet must still conform to the rules of contracting. As such, any amendment must not be unilateral, unless it was previously authorized by the other party. Therefore, the amendment should be recorded as a proposal pending its acceptance by the other party. Until such time as an amendment proposal is adopted, the contract must persist as was originally signed—in which time many proposals can be submitted in parallel. When an amendment proposal is finally found agreeable by all parties, it is then ratified into the contract, its execution to continue in the same state as the initial contract.

A similar such process would apply to early termination of a contract. So long as both parties can also agree on how to settle the remainder of the obligations—whether to waive them or to compensate appropriately.

2.9. Reporting

A full featured SC may also be equipped with a web service, meaning that it can behave as a website does—in fact it may appear as a website, or be displayed on a mobile application. As such, it has the capability to provide reports, including its:

- (1) particulars,
- (2) status,
- (3) event history,
- (4) other custom purpose specific information.

As an example, we can imagine an individual loan agreement. The SC could have its own webpage, which would give both parties a report on the loan:

- (1) its purpose, i.e. preamble;
- (2) its parties;
- (3) its particulars, e.g. interest rate;
- (4) its history, e.g. initial date, past payment dates;
- (5) interest vs. principal amounts paid; and
- (6) future payment schedule.

3. In Law

3.1. Note on Jurisdiction

This treatise is not intended as a comprehensive analysis for all or any particular jurisdictions.

Given the authors specialty, this paper will admittedly have a bias towards the application of English common law.

3.2. Are Smart Contracts Contracts?

The short answer is: yes... generally. The simple fact of using SCs does not redefine what constitutes a contract. Therefore, a SC could be found to not be contract in Law—just as a paper with terms and signatures do not necessarily constitute a contract.

As every lawyer knows, a contract is composed of:

- (1) offer,
- (2) acceptance,
- (3) consideration, and
- (4) intention.¹⁰

Short of any other vitiating factors, the SC would in fact be considered a contract in Law.

Interestingly, one can quite easily draft a SC lacking any of those elements. All previous examples could very well be proper contracts, but let's examine SC that would clearly not be contracts.

Let's imagine a SC that only composes one programmatic event, which is that whenever deposits are made to its wallet, it simply re-deposits them to another wallet. This, in TCP/IP terms, would be a simple redirect; or in programming terms: a wallet alias—presuming of course that the wallet it deposits to would be changeable via amendment.

Another imaginable scenario is that of a SC that does very much the same behavior as the previous SC only it splits the funds in half to two other wallets. This example is interesting as it could simply represent a partnership entity—in that the SC's wallet is that payable destination for the partnership's invoices. However, simply by looking at the SC alone, one could not necessarily determine whether it constitutes an enforceable contract.

Both examples above can be useful SC structures in business; anyone trying to do something of this sort with actual bank accounts would find it most difficult to convince either the bank, the accountant, the regulator that what one is intending on doing is proper. Nevertheless, the SC system left unfettered does not impose judgment—just as your computer does not—nor does it interpret beyond its concrete instructions.

3.3. Internal Dispute Resolution

One interesting use of SCs is the inclusion of arbitration procedures. Let's imagine that the parties agree on a specific person to be the arbitrator, and take it a step further and identify the person by his PKI certificate. When a notice of dispute is raised, the SC could conceivably be frozen pending a decision by the arbitrator. Such a decision could either resume the SC unaffected, or include an award encoded as an amendment to the SC.

Such baked-in resolution procedures may encounter legal issues, please refer to the discussion in part 9.

¹⁰W. E. Peel, *Treitel: The Law of Contract*, 12th Edition, Sweet & Maxwell 2007, Chapter 3.

3.4. External Dispute Resolution

Barring any such internal dispute mechanism that suits the parties in all cases, if a party ever escalates a dispute to an external authoritative body, such as an arbitration center or a court, the SC's records could conceivably be exported and put onto record. This would provide a convenient, objective view of the facts for the authoritative body's review and consideration.

3.5. Procedure

Of course, standard rules of procedure are not to be trumped; therefore, such evidence is still subject to examination—not to mention, it will require the need for a new breed of expert witnesses and cryptography forensics experts to provide explanations for the data and perhaps aid the authorities to verify and interpret the data appropriately; e.g. verifying identities, translating the code into human language.

4. Technological Variations

This section explores in technical—non-lawyer friendly level of—detail of the technology involved in building this type of system. The following concepts are important to understand the newfound technological implications to Law from part 5 that may lead to new policy considerations as discussed in part 6.

4.1. Infrastructure

SCs—as complex as they are—are only one component within the system. Just as a webpage is nothing without the underlying protocols and interconnected hardware infrastructure; SC's equivalent infrastructure is composed of:

- (1) a Smart Contract Platform (“SCP”), and
- (2) a Smart Contract Management System (“SCMS”).

SCPs are the interpreter and executor components at the top layer, depending on the design may include the SC storage module as well. More fundamentally, the SCPs involve also an underlying protocol layer for the cryptographic functionality that's needed for verifying identities and so on. In addition, it includes libraries for SC's use; e.g. email, cryptocurrency support libraries.

SCMSs, in contrast, are a superstructure around the SCPs that includes:

- (1) a full database of the parties' particular information;
- (2) event scheduling of SCs;
- (3) the SCs functional workflows, e.g. drafting, amendment and termination workflows;
- (4) finally, a front-end API or UI for user interaction.

At the time of this writing, there are no operational SCMSs; yet there are two competing SCPs in development: Ethereum¹¹ and Codius¹². Both offer varied approaches in their SCPs.

¹¹Ethereum is a platform and a programming language that makes it possible for any developer to build and publish next-generation distributed applications. Information available at: [www.ethereum.org]. Accessed 18 November 2014. For further information visit: <https://www.ethereum.org/pdfs/EthereumWhitePaper.pdf>, Ethereum White Paper, V. Buterin, *A Next Generation Smart Contract & Decentralized Application Platform*.

¹² Information available at: <http://webcache.googleusercontent.com/search?q=cache:http://codius.org>, accessed 18 November 2014.

4.2. Cryptography

Firstly, let's demonstrate how the SC can be signed by adding a "signature" at the end. Such could simply be an encrypted piece of data at the end of the SC's code whose meaning can only be revealed by the signatory; thus, the signatory is verified.

One can verify the signature so long as it is encrypted by one of the person's PKI keys. For example, let's consider that the signatory encrypts his signature with his private key; then anyone, using his publicly available public key certificate can decrypt and verify the signature as belonging to the signatory.

Conversely, let's imagine that the signatory chooses to encrypt the signature with his public key; then the data may only be decrypted by the corresponding private key. As such, the data composing the signature is meaningless and does not tattle the signatory's identity; nonetheless, when the signatory appears he may be verified by producing his private key.

Such are the two types of verification available to the parties: uni- or bi-directional identification; whereas one can make himself known openly on the SC, alternatively one can only make himself known by his own action.

Furthermore, the contract as a whole may be encrypted as to be meaningless to any outsider. This could guarantee privity of contract for jurisdictions that may not recognize the concept. However, it must be noted that the interpreter has to be able to decrypt the code to interpret it, obviously.

Lastly in passing, as an added level of security, by including and encrypting a hash¹³ of the code, one can ensure that the code was not tampered with.¹⁴

4.3. Decentralization

Codius mirrors more closely the current legal system, where an SCMS built on top of the Codius SCP would physically reside in a jurisdiction and would presumably be bound to it, unless otherwise stated.

Ethereum on the other hand, takes the idea of the Blockchain¹⁵—as established by Bitcoin—and applies it to the realm of SCs. The Ethereum SCP will take custody of the SC, placing it on its blockchain; hence, it resides everywhere and/or nowhere.¹⁶ Literally speaking, its custody is within a global consensus network, spread throughout countless computers across the Internet.

This decentralization of the SC makes for an interesting jurisprudential question: barring any express governing law clause, which jurisdiction would be said to be the seat of the contract? This issue is discussed further in part 9.

¹³The hash patent is publicly viewable at: www.google.com/patents/CA2441117C. The technology was invented by Silvio Micali.

¹⁴In oversimplified non-technical terms, imagine it as a hyper-compressed version of the code, from which the full code cannot be reconstructed, but the hash can be re-done and compared for authenticity.

¹⁵Available at: www.bitcoin.org/en/faq. Accessed 18 November 2014.

¹⁶*Ibid.*

5. Technological Implications on Law

Given the technology architecture as discussed above, absent new regulations, additional legal implications may arise.

5.1. Privacy

Pseudo-anonymity is an interesting concept; it ought not to be as intimidating a term as it sounds. A simple way to look at it, is to examine how email addresses do not in-and-of themselves reveal the identity of the person; only if one has the email registered in his own address book would he know who the person is. There is no centralized registration of databases and new, free emails can be created on a whim. The same is true of cryptocurrency wallets. The major difference is that wallets are not human-readable, to the point where one could perhaps not recognize his own wallet address. Otherwise, all is unchanged, the cryptocurrency wallet address is a one-way unique identifier that guarantees reaching a person's pocketbook, or inbox, but does not reveal the person's identity.

The issue surrounding this is rarely thought of, but is as follows: contracts are a heavily regulated exercise; much more so than the act of communicating—that is, in jurisdictions where speech is protected as a natural right. As much as speech may be protected, no jurisdiction allows full, unfettered right to contract—whether the contract be for: the sale of regulated goods, a criminal enterprise, or unconscionable pacts.

Jurisdictions will still inevitably attempt to crack down on such conduct. When SCs contain such illegality, courts will try to identify the party to the contract. This is where the difficulty will creep in; as wallet addresses will not inherently provide any clues to the party's identities. An additional consideration is the encryption of the body of the SC. The authorities may attach the SC via injunction, but neither its content, nor the parties' may be interpretable or identifiable without the parties' encryption keys. This presents a chicken-and-egg circular dependency in which there would be viable means to identify the parties, or interpret the content of the SC.

Some could leverage the opportunity to hide conduct—or involvement in such—from the public. This will inevitably come at odds with rights to privacy.

5.2. Jurisdictional

Along the same vein as the previous discussion on parties' privacy, the issues surrounding identifying the seat of the contract could be problematic to identify.

The major consideration will be, of course, the parties, the choice of governing law and the location in which the contract is being administered. There are no new issues here.

What is new however, is the possibility of having a SC administered by Blockchain Technology.¹⁷ What matters here is that the SC is not physically located, nor administered in any one specific physical location. In actuality, it is copied worldwide in a consensus network that guarantees its integrity. In a sense, it is both everywhere and nowhere.

Therefore, short of identifying the parties—which is not guaranteed—, or identifying the

¹⁷Ibid.

governing law—which may be encrypted and unreadable—, it may be quite challenging to identify a seat for the SC.

This could be seen as means for some to opt-out of public forms of legal systems. Given this, some could take the concept one step further and try to create new underground norms of contract law.

Such SCs without seat are technically possible with current technology on Ethereum.¹⁸

6. Policy Considerations

6.1. Banking, Regulatory and Fiscal Policies

The first effect of cryptocurrencies is the enabling of banking services¹⁹ outside of the scope of banking law.²⁰ This is because there is no need for banks in cryptocurrencies.²¹

Examining the evolution to the publishing industry that came about from the advent of the Internet. Here we have a global platform where anyone can be a publisher. It didn't outright kill the industry, but it certainly forced it to evolve—as has been observed since.

We should expect the same evolution to happen in commercial banking. The storage and transfer of funds services, given better user-friendly applications, in a cheaper, faster more convenient format, will challenge the *status quo* of commercial banks. The banking system will either evolve to rival cryptocurrency convenience, or will fall by the wayside.

There are important policy considerations here, for:

- (1) banking,
- (2) regulatory, and
- (3) fiscal policies; as of these would be impacted if a critical mass of the public would stop using public banking systems.

Firstly, banking law has evolved for centuries and is quite entrenched in our current legal system. It serves as means for:

- (1) consumer protection against unfair practices;
- (2) prevention of fraud;
- (3) general rules of order; and finally
- (4) public aggregate reporting.

Secondly, banking and financial regulation has for its goal of:

- (1) consumer protection against unfair practices;
- (2) risk controls; and
- (3) prevention of fraud.

Thirdly, fiscal policies with which governments see it fit to regulate the economy, typically by

¹⁸Information available at: www.ethereum.org, accessed 18 November 2014.

¹⁹Banking services are generally referred in law as that of accepting current accounts and paying in and paying cheques for the bank's customers. *Foley v Hill* (1848) 2 HL Cas 28; *Joachimson v Swiss Bank Corporation* [1921] 3 KB 110.

²⁰Both statutes and common law.

²¹Available at: www.bitcoin.org/en/faq, accessed 18 November 2014.

means of: (1) regulating interest rates; and in some cases, bail-ins²² and bail-outs²³.

Firstly, banking law and banking regulation require bankers to follow some procedures. In the cryptocurrency world, there is no need for banks, as previously established. Therefore, such rules would become obsolete. Furthermore, should there be a massive move towards the use of cryptocurrencies, to the detriment of traditional banking systems, public authorities would stand to lose public aggregate banking statistics, which would make fiscal policy not only difficult, but ultimately ineffective as fiscal policies would not have any provable direct impact on cryptocurrencies.

6.2. Financial Unleashing

The impact that SC can have in addition to the cryptocurrencies' impact on banking is even more profound.

Given the previously discussed concepts, we now see that a new, larger shadow banking system is easily possible.

This will either be very good for investment banks, or very bad for them. Firstly, this will provide the financial industry with more tools with which to scale existing, legal financial products, as well as also facilitate regulatory arbitrage²⁴ to avoid local regulations.

This will pose a serious challenge to local regulations, and exacerbate the economic competition between jurisdictions; as the moneyed elite will more easily be able to jurisdiction-shop for friendlier locales.

The other consideration is that SCs can allow for more sophisticated financial products, the likes of which would not otherwise be possible, either given technical or regulatory restrictions. Such innovation is likely to produce more cyclical economic fluctuations; the difference here will be that attempts for additional regulations may be ineffective.

As financial products become more popular, it becomes possible for the products to become standardized SCs, and hence be easily reproducible by the less moneyed classes.

Ultimately, either voluntarily or otherwise, it is likely that financial services will be unleashed, either by voluntarily deregulation or by reluctant desperation. At such a point, a nation's ability to regulate fiscal policies would become very difficult, short of banning cryptocurrencies altogether.

²²Name commonly given for heavy handed public correction of financial crises; e.g. Troubled Assets Relief Program ("TARP"). As an example, the US Treasury established several programs under TARP to help stabilize the U.S. financial system, restart economic growth, and prevent avoidable foreclosures. Information available at: <http://www.treasury.gov/initiatives/financial-stability/TARP-Programs/Pages/default.aspx>.

²³Name commonly given for mass seizures of bank accounts for purposes of public correction of financial crises; e.g. the Cyprus Bank Crises of 2013. For more information, visit: <http://business.time.com/2013/03/21/cyprus-banking-crisis-the-endgame-begins>, P. Gumbel, *Cyprus Banking Crisis: The Endgame Begins*, Business Time, 21 March, 2013.

²⁴Name commonly given to a strategy in which a venture is located or re-located in a jurisdiction with a friendlier regulatory environment. A. Shleifer, R. Vishny, Robert, *The limits of arbitrage* (1997) Journal of Finance 52.

7. Criminal Activity

7.1. Potential Uses

Most unlawful activity attributed to Bitcoin is generally not new to cryptocurrencies; e.g. money laundering, theft. The only new aspect is the speed and efficiency with which such activities could be done. However, one must consider that, using Bitcoin specifically—with its use of a public, permanent ledger—it is not a good tool for criminal activity as it can tattle the rogue’s behavior long into the future. This is not so true for all cryptocurrencies however; such as is the case for Darkcoin²⁵, which is specifically purposed to anonymize the economic behavior of its users.

Smart Contracts, on the other hand, are similar in that they do not offer new means of criminal activity—no more than “dumb” paper contracts could. However, in the same vein, one must ensure that the contract represented in the SC is in accordance to law. This is of course a larger discussion as such issues that cross all categories of law, across all jurisdictions.

There is one more consideration, however, that is the possibility to make the SC illegible via encryption... but again, not very dissimilar to encrypting a paper contract.

7.2. Mitigation

Given an SCMS, its interpreter component must at all times be allowed to interpret the SC’s code in order to interpret it, obviously. Due to this technical limitation, the SC must be decryptable by the SCMS. As such, a regulatory body could compel, or impose an injunction on, a SC to be revealed to public authorities.

It is likely that this issue will be discussed in legislative bodies in the future to regulate SCs. As such, it is likely that in some jurisdictions, SCMSs will be regulated to allow public authorities to seize SCs.

8. Regulation

8.1. Legislative Position

The current legislative position, at the time of this writing, is quite simple: it has never been discussed in legislatures. The reason is that, of course, this discussion is pre-emptive, as SCs are not currently publicly available as a product or service—although, there is beta version software available to demonstrate the technological concept.

It may be inherently illegal, same as cryptocurrencies are illegal due to inflexible laws on legal tender; some jurisdictions may have inherent laws similarly prohibiting SCs.

8.2. Lobby

There is a long held tradition of crypto-anarchists²⁶ that are increasingly active in their lobbying for privacy and online freedom. There is a spectrum at play here. We firstly observe, on the public legitimate front, strong lobbying efforts by groups, such as the Electronic

²⁵Darkcoin is an open sourced, privacy-centric digital currency. It allows users keep their finances private as users make transactions, similar to cash. Information available at: www.darkcoin.io, accessed 18 November 2014.

²⁶C.f.: the cryptoanarchist manifesto, please see: www.activism.net/cypherpunk/crypto-anarchy.html.

Freedom Foundation²⁷ that argue invariably in favor of freedom and privacy. On the darker side, there is Anonymous²⁸, whilst an illegitimate activist group also invariably takes on the side of freedom and privacy; albeit, in what could arguably be terrorist tactics.

The point here is to underscore the concept that there is likely to be an escalating-arms-race between the white-hat authorities and the cryptoanarchists. This will be played out in the realm of the darknet²⁹, where there are black-market activities; e.g. sales of illicit material, or illegal drugs. The darknet will presumably make use of SC related technologies and apply strong cryptographic obfuscatory measures; conversely, the authorities will escalate the sophistry of their measures to catch such actors.

9. Apparent Issues

There are many issues that can be raised, but upon further analysis reveal themselves to be non-issues.

9.1. Bugs

A major, valid concern is the possibility for there to be bugs—i.e. unintended behavior—in the SC's code. Upon reflection, one could easily argue that this is not a new issue, as unintended clauses in code is quite common and is generally known as a “loophole.”

This is a more severe concern in SC's case as there is:

- (1) fast performance via automation;
- (2) use of non-human-readable code; and
- (3) use of large code libraries, which could include vast amounts of implied code.

In such a situation, one hopes that the SCMS has a rollback mechanism or that the parties can rectify the situation; otherwise, the aggrieved party will have to seek remedy in the usual means.

9.2. Is it a Trust?

A SC is often compared to a trust³⁰, in the sense that the SC is the trustee³¹ performing for the parties holding the role of both settlors and beneficiaries; whereas the code is the indenture

²⁷The Electronic Frontier Foundation is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, Electronic Frontier Foundation champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. The Electronic Frontier Foundation works to ensure that rights and freedoms are enhanced and protected as the use of technology grows. Information available at: www.eff.org, accessed 18 November 2014.

²⁸Information provided by The Guardian on Anonymous can be found at: <http://www.theguardian.com/technology/anonymous>.

²⁹Name commonly attributed to Internet activities and forums conducted in ways that are difficult, if not impossible, to trace. Darknet is a group of individuals founded around 1999 sharing knowledge in password cracking, cracking, cryptography and programming. Information can be found at: <http://www.darknet.org.uk/about>.

³⁰The basic idea of a trust is that the legal and equitable property in an object is separated and are placed with different persons. The person who holds the legal property is put in a fiduciary duty towards those who are placed with the equitable property. Scott, Austin, *Importance of the Trust*, 39 University of Colorado Law Review 177 and H. Hansmann, U. Mattei, *The Functions of Trust Law: A Comparative Legal and Economic Analysis*, New York University Law Review 1998, May.

³¹Trustee denotes the party that holds the legal title or property but is put within the fiduciary duty of the equitable property holder – the beneficiary.

and the holdings of the SC to be its res. For jurisdictions³² where trusts are indeed recognized, this is generally not applicable for SCs, as a trustee must be a natural or legal person with the capacity to contract.³³ Until such time as SCs are recognized as legal persons, this will not be the case. A discussion on personhood is detailed below.

Although this is not the case, would a SC ever be considered a trust could bring interesting implications, such as the applicability of Trust Law.

9.3. Is it an Agent?

What if one could encode a SC to engage in other contracts? Then the issue is whether the SC can perform as a legal agent³⁴—i.e. to have the capacity to be authorized to contract on behalf of another (natural person).

Again, as per the trust scenario, the general position in law is that only natural or legal persons have the capacity.³⁵ Barring such a declaration of status, this is not the case. However, this will be discussed further in the next section.

9.4. Is it a Person?

As previously alluded, at some point it may be argued that SCs are legal persons³⁶, in the sense that they are:

- (1) identifiable,
- (2) have a capacity for rights, and
- (3) capacity for obligations.

As previously established, a SC can be considered to meet the criteria:

- (1) identifiability from its cryptographic identity;
- (2) capability to exclusively receiving and controlling—i.e. to exercise all ownership rights over—digital assets;
- (3) capability to independently perform contractual obligations.

There is an additional interesting argument to be made however. Many financial institutions, as well as private traders, construct software that—via an heuristic method—makes lightning quick decisions on, and places trades to market exchanges. This could easily be argued that this is standard practice as it is so widespread; indeed, halting its practice suddenly would severely impact the financial health of developed economies. Therefore, one could argue on a policy basis that software ought to be recognized as an agent implying its personhood.³⁷

³²Common law jurisdictions recognized the concept of trust, while generally, civil law jurisdictions do not. H. Hansmann, U. Mattei, *op. cit.*

³³It is understood and generally discussed in many contract textbook that only ‘people’ have the *sui juris* to enter into a legally binding contract. Contract law provides protection to those who do not have or do not have full legal capacity to enter into a contract by invalidating them. Some of these categories are: a) minor; b) the mentally incapable; and c) drunkards. L.A. Kornhauser, W. Bentley MacLeod, *Contracts between Legal Persons*, NBER Working Paper No. 16049 Issued in June 2010. Available at: <http://www.nber.org/papers/w16049>.

³⁴F. Andrade, P. Novais, J. Neves, *Will and Declaration in Acts Performed by Intelligent Software Agents - Preliminary Issues on the Question* [in:] *Proceedings of The 4th Workshop on the Law and Electronic Agents* (LEA 2005), pp. 53-55; see also: G. Sartor, *Agents in Cyberlaw*; A. Yip (2002), *Some Issues on Agent Ownership* and A. Artosi, *On the Notion of an Empowered Agent* [in:] G. Sartor, G. (ed.), *Proceedings of the workshop on the Law of Electronic Agents (LEA02)*.

³⁵The idea of capacity is similar to that in contract law.

³⁶The concept of a legal person is that it is not a human being entity, but it is treated as a person for certain limited legal purposes, e.g. Smith, Bryant: *Legal Personality*. (1928)Yale Law Journal 37 (3): 283–299

³⁷For a fuller discussion and arguments on the application of rights and personhood on non-human subject, see C.

An even simpler scenario shows that automated systems are already in the business of contracting, such as the case of a vending machine. If the argument would to be made that only persons can engage in contracts, then this would imply that the vending machine's contract would not be binding. As a matter of convenience, this has become standard practice, but this still stands in a lacuna in the law.

As things stand, the granting of personhood status is generally only recognized by official declaration—which has yet to be conferred in any jurisdiction.

10. Legal Issues

This section discusses the issues raised by SCs for which there is no clear authority and are arguable either way.

10.1. UPL

The first issue to consider is whether drafting and/or advising on SC constitutes practicing law.

Most jurisdictions empower their law society with a monopoly over the practice of law in the state and generally has discretion over the granting of law licenses. As such, if one is deemed to be practicing law without the said license, then one can be found guilty of Unlicensed Practice of Law (“UPL”).

To examine this, we may look back at whether drafting or advising on traditional paper contracts requires a license. However, there is the additional complication in that SCs run on SCPs and SCMSs; therefore, an additional issue is whether advising on which SCP/SCMS to use, or advising on SCP/SCMS specific optimizations, be also considered practicing law.

The final issue relates to who is the custodian of the SC. The SCMS must be maintained by a person. Given the security risks associated with the custodial responsibility of SCs, an argument could be made that sufficient insurance ought to be imposed by regulation. Therefore, it is conceivable that the very act of running and maintaining an SCMS could be a licensed activity.

10.2. Licensed Business Activities

Some activities are licensed as a business, which are otherwise legal if done in one's private capacity. This obviously depends on the jurisdiction, but for example, many jurisdictions outlaw sports betting businesses, but allow private individual sports betting.

SCs allow mass-production of one-on-one contracts to the scale of a business, where a business could position themselves as simple being in the business of selling pre-defined SCs —e.g. a sports bet contract, to follow the previous analogy. This most probably simply skirt the purpose of the legislation, as presumably such rules were enacted to prevent mass-adoption of the activity with minimal oversight. SCs, coupled with the wide reach and convenience of the Internet, threaten to disturb the current balance of some licensed business activities by lowering the barriers to enter the business.

Wellman, *Real Rights*, Oxford University Press 1995.

The issue that arises is whether such a person that is in the business of selling specialized SCs that represent a legal activity as individuals—but is otherwise a license business activity—is in violation of said license. This will obviously be a matter of interpretation, but may force legislatures to either clarify or tighten their definitions of what constitutes acting in the said licensed business.

More examples of businesses that are usually licensed, but could be mass-produced with the use of SCs are: loans, betting, lotteries, stocks/bonds/derivatives exchanges, derivatives, insurance, etc.

10. 3. Regulatory Difficulties

Interestingly, if we imagine a scenario where Peer-to-Peer securities exchanges become easy to instantiate³⁸, then the amount of oversight required to police such activity, coupled with the ease with which one could side-step the long arm of the law either by going off-shore, hiding the identity of the parties, and hiding the seat of the contract. This would inevitably cause some to re-evaluate whether such licensing standard are worth maintaining.

11. Political Issues

11.1. Risks

In order to appreciate the rationale behind any legislation, we must first understand the potential risks to the state. Since SCs hold personal information, there is an obvious privacy risk from having its data being leaked. Beyond this, to have all of one's SCs to be leaked would also tattle one's whole business, which is an even more severe risk as it could be very valuable to one's enemies or competitors—more so than the personal data.

Further risks are not to the individuals but to the economy at large. As discussed in part 6, fiscal policy is means for the state to regulate and normalize the economic environment. This is done by imposing controls, not only by the Central Bank, but also on the banking and financial systems—collectively composing the spigot of the economy.

An additional reason for regulating the banking system is to allow oversight on the aggregate economic indicators and statistics, without which data-based fiscal policy making would be much more difficult, if not impossible. Furthermore, the ability to regulate banking is important for enforcing judgments and interlocutory measures, such as injunctions on accounts. A Bitcoin wallet cannot be attached, but a SC could if the SCMS is a licensed entity.

11.2. Licensing

The first political issue will certainly be whether to regulate SCMSs. There are several reasons why states may want to regulate them:

- (1) legal advice is necessary is the general case in drafting SCs;
- (2) requiring legally compliant workflows in managing the life-cycle of a SC;
- (3) managing the security risks related to the assets held by the SCs;
- (4) requiring access by public authorities.

³⁸Such as cryptocurrencies as easy to create your own. which is should in Bit Clone, available at: www.bitclone.net.

Therefore, it is quite likely that some jurisdictions will choose to regulate SCMSs. The options to consider are as follows:

- (1) imposing insurance requirements;
- (2) imposing reserve requirements;
- (3) requiring approved security audits;
- (4) requiring a law license; and/or
- (5) including a process for public authorities to enforce injunctions.

11.3. Oversight

Another issue is whether an SCMS is an implied trustee, similar to how a banker,³⁹ who ordinary⁴⁰ legal status may change and could be considered in the position of a constructive trustee.⁴¹ Such concept was put in place with the rationale that bankers should somewhat be responsible to prevent fraudulent activity by their customers through the banking systems.⁴² I.e. should the SCMS make it its business to prevent illegal activity? One could argue that the SCMS has a public duty—being the one in the best (if not the only possible) position to do so—to oversee SCs’ legality.

As such, one could foresee that the polity might see it fit to make an SCMS an exclusive public service supported by public funds—much like courts are today.

Alternatively, SCMSs could be compelled by the state to open the records for public authorities ostensibly to monitor for terrorist activity—much like Internet Service Providers, banks and telephone systems are often monitored.

12. Conclusion

12.1. Trends

At the time of writing, there is no publicly available production-ready SCMS, or even SCP. There are some beta versions available with which to tinker. The most long-lived project is Ethereum⁴³, which has notably raised at most US\$15M⁴⁴. Other notable projects in

³⁹The terms ‘bank’ and ‘banker’ may be used interchangeably by legislations (as an example, the Bills of Exchange Ordinance (Cap. 19) and the Banking Ordinance (Cap. 155) in Hong Kong) and courts, they are usually not inconsistent with each other. Even status’ definition of a ‘bank’ generally refers to the procedure nature, the protections and common law definition of ‘banker’ will still apply. Roebuck, Srivastava, Zafrullah & Tsui, *Banking Law in Hong Kong, Cases and Materials*, 2nd ed., LexisNexis 2009, p. 26.

⁴⁰A banker is considered a banker in common law if it shows that:

1. it holds current accounts for customers;
2. its customers can draw cheques from the bank; and
3. it collects cheques on behalf of its customers.

If a banker shows the requirements in common law, the ordinary relationship the bank has with its customer is one of contract, with an addition requirement to honour its customers’ cheques. As explained in the House of Lords decision in the case of *Foley v Hill* (1848) 2 HL Cas 28.

⁴¹The concept of constructive trustee was laid down in the case of *Barnes v Addy* (1874) 9 Ch App 244. The court held that a stranger who acts as an agent of a trustee can, in law be held to be liable as a constructive trustee, if that agent assisted in the dishonest and fraudulent conduct of the original trustee with knowledge.

⁴²In the case of *Selangor United Rubber Estates Ltd v Cradock (No. 3)* [1968] 1 WLR 1555, the principles were adopted into a bank and customer situation even the application of the principles were slightly toned down in a later Court of Appeal case of *Lipkin Gorman v Karpnale Ltd* [1989] 1 WLR 1340.

⁴³Available at: www.ethereum.org www.bitcoin.org/en/faq, accessed 18 November 2014.

⁴⁴R. Mcmillan, *Project to Turn Bitcoin Into an All-Powerful Programming Language Raises \$15M*, 9 Oct 2014. Available at: www.wired.com/2014/09/ethereum-backers-raise-15-million.

development are: Codius⁴⁵, CryptoLaw⁴⁶, BitHalo⁴⁷ and CounterParty⁴⁸.

12.2. Looking Ahead

Both Ethereum and Codius have indicated that they expect to be production ready by 2015. Whether they both deliver on schedule or not, one should expect that this technology ought to be publicly available before 2016.

12.3. Comment on Existing Regulation

As mentioned above, the authors very much expect legislatures to eventually face the issues introduced by SCs. The authors wish to encourage a balanced and durable long-term approach.

In order to do so, one must consider the sufficiency of existing law in addressing what appears to be new criminal behavior but are simply new manifestations of old crimes. Examples of this could be of hacking someone's cryptocurrency wallet. This is not anything more than an unauthorized access crime, or otherwise put: a trespass, as well as a theft.

For enforcement to be handled appropriately by authorities, there obviously needs to step up Blockchain technology based forensics and evidentiary procedure.

Furthermore, another consideration for legislatures to consider is the coming ineffectiveness of law enforcement that is bound to happen from increased technological efficiency that will lower barriers for the public to engage in licensed activities—similar to how ostensibly illegal downloads of copyrighted material became prevalent due to ease around the turn of the century.⁴⁹ The lesson to be learned here is that when an activity is so easy to do yet so difficult to enforce, the trend can lead to the activity becoming so prevalent that enforcement becomes near impossible, both physically and politically.⁵⁰

The legislature will be faced with a choice: either to scale up, at significant expense, the efforts to prevent the prevalence to reach critical mass; or to scale down regulations. As much as the latter may seem as a resignation—a win for the mob—it could also be seen as recognition of the people's will to decriminalize such conduct.

Obviously, the legislatures will have to balance their values and principles in reaching their decisions; but one may hope that they reach a balanced, long-term view lest they ratchet up public force only to fight a losing battle.

12.4. Comment on Future Regulation

Lastly, the legislatures will also have to discuss whether SCs, SCPs and SCMSs are to be controlled via licensing.

⁴⁵ Information available at: <http://webcache.googleusercontent.com/search?q=cache:http://codius.org>, accessed 18 November 2014.

⁴⁶ Information available at: www.cryptolaw.com, accessed 18 November 2014.

⁴⁷ Information available at: www.bithalo.org, accessed 18 November 2014.

⁴⁸ Information available at: www.counterparty.co, accessed 18 November 2014.

⁴⁹ G.M., *The legacy of Napster A tale of two file-sharers*, 13 Sep 2013, The Economist. Available at: <http://www.economist.com/blogs/prospero/2013/09/legacy-napster>.

⁵⁰ Ibid.

The first issue to determine is whether advising on SCs constitutes practicing law. If so, then that activity would be included within the purview of the state law society. Either way, there will most probably need to be some clarifications and/or amendments made to the applicable law.

The second issue is to determine whether administrating SCs, i.e. running an SCMS, also ought to be a licensed activity. This is a new concept with which is difficult to bring a real world analogy. Therefore, this issue requires a fresh look.

12.5. Suggestions

In conclusion, the authors' suggestion to legislatures is to extend the current intent of the definition of what constitutes practice of law to its congruent construction in order to accommodate advising on SCs. When it comes to administrators of SCMSs, it is reasonable for there to be some minimum level of risk controls, such as insurance; or a reserve requirement in proportion to the digital assets under control of its SCs.

12.6 Takeaway

The authors hope that this paper has educated the reader in this new (not even yet fully developed) technology. As much as we would like to take credit for the predictions made herein that may eventually come true in the future, we must hedge against some not coming true by reminding the reader of what the future looked like in the mid 90s.

When the Internet was in its infancy, one could scarcely predict the rise of Google, Facebook. It was a time where only a few were even aware its existence or its technological feasibility; even amongst those who were, many could not see its utility.

We are in the same period, just like the early 90s on the Internet: where technological issues are not yet ironed out, where its use is limited to academic exercises and where only pure enthusiasts endure the clumsiness and user-un-friendliness.

That said, we can only imagine where the future of SCs will take us.

Samuel Bourque is a JD student at City University of Hong Kong, School of Law, Tat Chee Avenue, Kowloon Tong, Hong Kong and is a software engineer

Sara Fung Ling Tsui is a Teaching Fellow at the School of Law of the City University of Hong Kong, Tat Chee Avenue, Kowloon Tong, Hong Kong. She is also solicitor of the High Court of Hong Kong SAR.

Contact e-mail: lwsarsa@cityu.edu.hk