Blockchain vs. Trust: Cryptic Expert Issues

by Dr Stephen Castell CITP MIoD MEWI*

A presentation for *The Reg A Conference*, New York City, June 12, 2018**
(Or similar: 'Does Your Company Need Funding?')

Abstract

The Reg A Conference is the largest gathering of deal-makers and investors interested in Regulation A, a prime opportunity for companies to network with like-minded business executives, as well as financial professionals who assist in bringing capital to companies (https://theregaconference.com/presenting-companies/). Many such companies are today basing their new business ventures and projects, and their search and submissions for funding, on blockchain technology applications. So-called cryptocurrencies such as bitcoin are just one example of the use of this functionality. The business implications of this secure online record-keeping tech are huge – and not only in cryptocurrency. This presentation provides a probing and extensive expert critique of blockchain, its cryptocurrency, distributed ledger and smart contract applications, and argues for a cautionary, savvy approach to implementing and investing in such business systems, on grounds of professional due diligence, rigorous corporate governance and wide experience of past leading-edge ICT systems failures.

Some Technical Background

The blockchain is a digital shared public ledger on which a 'cryptocurrency' (e.g. Bitcoin) network relies. It has a linked list data structure, with each block containing a hash of the previous block. Each block is formed by a proof-of-work algorithm, through which consensus of this distributed system is obtained via the longest possible chain. The blockchain provides the basis for the 'trustless distributed system' of a cryptocurrency and it is extendable in many ways through modifications of the parameters of the chain.

A block is an aggregated set of data. Data are collected and processed to fit in a block, each block identified using a cryptographic hash (or digital fingerprint). The block formed contains a hash of the previous block, so that blocks form a chain from the first block ever (known as the Genesis Block) to the formed block. In this way, all the data are connected via a linked list structure.

A 'traded' cryptocurrency blockchain (e.g. Bitcoin) is a shared public chain: in principle everyone has access to the chain, not only to read the information on the chain, but also to append new blocks on the chain. This is known as an unpermissioned chain.

However, for blockchain applications other than cryptocurrencies, the chain can be modified for stricter access control, the strictest being that of a private chain, where only the owner of the chain has full access to the chain, others having no access at all, similar to the way a central database stores confidential data. In many real-world financial and business applications, or 'use cases', a system somewhere between a shared public chain and a private chain is likely to be appropriate. Through public key cryptography, access control can be implemented during setting up of the chain so that differentiated access controls could apply. An example would be the health information of an individual; another, the product reference and customer/supplier transactional details of supply-chain management. These could be set up to be accessed only by the 'data subject' (patient, procurement manager) or anyone granted access by that subject – only a trusted body could append new data to the chain. This is known as a permissioned chain. Investors are most likely to be involved in funding new permissioned chain start-up applications.

Crypto: the Millennials' Rock'n'Roll

> "*Blockchain technology introduces permanence and immutability into the digital world. … Three aspects are needed to build a modern society. The first is memory. … The second is communication. … The third component, which underpins the other two, is trust. … everything runs on trust. We trust our banks to keep our money safe. We trust Google with our personal and work emails. We trust the courts to make unbiased decisions and keep proper records. Memory and communication are of limited use in the absence of trust.*
> *For the most part, this trust is not misplaced. Banks and courts are highly regulated entities … But this trust is still a human affair, and hence regularly betrayed. … trusts costs money—we pay these institutions a trust tax, which in practice translates to thick legal agreements and insurance premiums. …*
> *Enter blockchain. Blockchain is the technological revolution that commoditizes trust … by integrating trust on an infrastructural level into any service built on blockchain. Trust normally has to be enforced via laws, courts, armies, and other costly, fallible institutions. Replacing these with disinterested cryptography promises a revolution in the way we enable trust. …*
> *[This brings up] the right to be forgotten. A law that grants individuals, under some circumstances, the right to demand of websites that they remove information about themselves. However, in a distributed consensus system like blockchain, enforcing the right to be forgotten becomes technically impossible. …*
> *As technology becomes part of our extended mind, the right to be forgotten can be construed as tantamount to memory manipulation. You might think that this is an important and necessary thing we have to do in order to protect social harmony, or you might loathe it as an entrenchment on your individual freedom. Blockchain technology, however, has no opinion. It takes no ethical stance. It protects our collective memory from adulteration, ill-intentioned or otherwise, with no regard for whatever the consequences may be. …*"
> Júlio Santos, November 14, 2017 **[1]**.

It is difficult not to notice the vigour and pizazz of the current mania for *Crypto-Algorithmic Blockchain Technology* and it is a fair bet that there is far more being written about, energy going into, and money being invested in (gambled on?) Bitcoin and other cryptocurrencies, blockchain, smart contracts and distributed ledger technology than even into Artificial Intelligence (AI). Almost every other person you run into, particularly if a Millennial, seems to be involved with an Initial Coin Offering (ICO) or Initial Token Offering (ITO). With just a 'White Paper', little or no investment due diligence, and taking advantage of a regulatory vacuum, this 'Crypto Tribe' are raising billions in real legal tender, 'fiat currencies'. This substantial finance-raising is being used to fund fantasy coins and tokens – with no more obvious or established economic utility or asset value than, well, a bar of gold – in the hope of developing and successfully launching a plethora of brave new business and social ideas, products and services, heralded by enthusiasts as a whole new 'crypto-economy'. **[2]**

No doubt a few of these will prove to be commercially-successful, reputable, significantly disruptive game-changers, and usher in the possibility of some sort of new – trusted – global 'crypto-economy' paradigm. But at the moment, one can be forgiven for believing that most ICOs/ITOs, cryptocurrency 'mining', and crypto-coin trading exchanges have already been largely taken over by the 'black cash' of drug-dealers and the like, and in a substantive not-easily-reversible way.

Many of the Millennials, let down after the post-2008 credit crunch by governments, the banks, and educational system, and, it appears, largely not needing to be subject to Know Your Client (KYC) and Anti-Money Laundering (AML) strictures, may not be too worried where they get their ICO money from, or how it is actually going to be (accountably) spent, or whether that will result in a viable business. Nevertheless, and leaving aside the fraudsters and money-launderers, I wish these crypto-enthusiast Millennials well.

Indeed, I have dubbed 'Crypto' the *Millennials' Rock'n'Roll*. Some of us were lucky enough to have lived through the exciting birth of the Real Rock Thing, sixty years ago and, still regularly feeling its enduring foot-tapping tingle, I simply say: *Rock On, Millennials*!

I myself suggested, over thirty years ago, just such a new, disintermediated wholly digital cash currency, in a letter published in July 1995 in *Computing* magazine:

> "*... As cybertrading grows, the new, powerful common electronic trading currency will be 'owned' by no single physical nation state, central bank institution, economic or political grouping. We could even call it the ECU. Not the European Currency Unit, of course, but the Electronic Cash Unit*".

And, long before the Millennials were even born, in a fictional article, '*Ye Nom De Das Geld*', in the December 1971 issue of *GONG* (the student magazine of the University of Nottingham) I went even further with my conceit of a 'Post-Purse Paradise':

> "*Brother and sisters, I welcome you to the post-purse paradise. ... Geld is in heaven, all's well with the world. ... Cromstock and I first mooted the possibility of an Economic Reformation taking place in Britain in The Journal Of Comparative Economics during ... 1969. ... to put into practice ... the tenets of the Quasicurrency Theory which I had been formulating over the preceding twenty-five years. ...* " **[3]**.

It may well be that many, probably most, of the current species of cryptocurrencies, currently digitally 'materialising' daily, as if by magic, through one ICO or another, will fade away, and/or at some point be regulated out of existence. Blockchain applications generally however are undoubtedly here to stay. The majority of these will be serious, robust implementations, by established major corporations, with most of us, as consumers, hardly needing to know about the technical, legal or operational details. It seems clear that, within a few years, an extensive settled, but vigorous and continually innovating, 'blockchain applications industry' will be in place, one bearing little resemblance to the frantic cryptocurrency 'bandit territory' landscape of today.

Blockchain: Sceptical ICT Professionalism and Legal Due Diligence

As an ICT expert and professional I am however duly cautious about this newly unfolding 'crypto-economics' blockchain landscape. This caution is a proper part of being a skilled professional applying knowledge and experience to assess the most appropriate tools and technologies for a given (business or other) application's requirements. The savvy ICT expert bears in mind, for example, not only that there are no finalised international/ISO standards yet for blockchain (eight standards are in development under ISO/TC 307), but also there is far more to specifying, designing, developing, testing, deploying and maintaining an appropriate complete QA-assured system than just 'the blockchain bit'. And whether to use blockchain as a component *at all* for a given business/system requirement is of course a critical feasibility exercise that the seasoned professional will know is essential.

It should be no surprise if a diligent ICT systems engineer may conclude, on an experienced expert assessment, that many things can be achieved just as effectively by other means. He or she will carefully and responsibly consider all the pros and cons to ensure that the non-expert customer/client/investor/employer (to whom a professional fiduciary duty is owed) gets the most suitable, 'fit for purpose', secure, robust and performant system available, and takes properly risk-assessed competitive advantage of any new developments in technologies, tools, methodologies and processes (and always consistent with the budget/price willing to be paid, of course) **[4]**.

Furthermore, the legal status of cryptocurrency, smart contract and distributed ledger technology is not clear, or uncontentious. In the USA, there is already ICO litigation on foot. **[5]**. Having been involved in advising on ICOs, prior to launch, I have encountered some significant tensions and challenges between the crypto-enthusiastic, blockchain technical specialist, and the sober business development objectives of, and the professional due diligence to be done for, the putative ICO-issuing company owner or managing executive.

Consider, for example, this scenario: a highly proficient, high-profile, software engineering entrepreneur and thought-leader, let us call him Joshua, a US citizen, reckoned by many to be one of the most experienced, and imaginative, technical and regulatory experts in the blockchain and cryptocurrencies field, is in the process of developing and launching various Initial Coin Offering ventures and services. Joshua asserts "nobody knows more about how to do this work in the right way, in compliance with every single rule and regulation, than I do". In particular, there is a substantial going-concern OTC-listed company, let us call it XYX-CAP, Inc. ('XYX-C'), which is poised to do an ICO, designed, led, promoted, launched and actioned-to-market by Joshua.

The following queries and issues arise:

(1) If the XYX-C Coin created by this ICO is likely to be deemed by any relevant (US or other) regulatory or law-enforcement authority to be 'asset-backed', and for that reason (or, indeed, any other) equivalent to *issuing a security*, would it not be advisable, 'just to be safe', to *seek securities regulatory approval for this ICO before it is publicly launched*? If so, what exactly is the relevant and correct 'securities regulatory approval' to be sought, with whom, where, etc and how does one go about that, correctly, accurately and timeously?

(2) Joshua says "*It's very important to be aware that this is an open community blockchain project. This necessarily involves launching something that will have the XYX-C name attached to it in perpetuity, but giving up exclusive control of what it becomes*". If the CEO of XYX-C is not wholly comfortable with this, are there any sensible steps that XYX-C can take to protect its name, brand and trademark to counter (or at least ameliorate) 'giving up control of what it becomes'? If so, what, and how, and at what cost to put it in place?

(3) Suppose this ICO goes badly wrong at some point, and either the XYX-C company, or the public at large investing in the XYX-C Coin, claim they have lost money, or otherwise been damaged by taking part in its launch, and also claim that Joshua, and/or I, made misrepresentations, and were negligent/fraudulent, and thus seek reparation from or, worse, criminal prosecution of, us, what can he and I do to avoid, or protect against, that possibility, or its consequences, *at the outset*, i.e. *before* the ICO is launched publicly? Are there any sensible legal and practical protective steps we can take? **[6]**

The 'Right to be Forgotten'

Sceptical ICT professionalism and legal due diligence apart, the 'Right to be Forgotten' may in and of itself be something of a barrier to the ubiquitous introduction of computer and communications systems applications based on cryptographic blockchain software and technology. The General Data Protection Regulation (GDPR), in force from May 25, 2018, includes in its provisions Article 17:

> http://www.privacy-regulation.eu/en/article-17-right-to-erasure-'right-to-be-forgotten'-GDPR.htm

> *"Right to erasure ('right to be forgotten')" ... (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; …*

In my analysis and view, blockchain, with the 'permanence and immutability' of data records written to the blockchain as a critical, fundamental, key feature, is potentially likely to be structurally unable to be compliant with Article 17, Right to Erasure, of GDPR.

There is a view that, in regard to interpreting and implementing 'erasure' in practice, simply 'putting data beyond use' electronically satisfies the standards for GDPR data privacy. This would mean that, for example, setting record 'delete' flags, 'losing' cryptographic keys, or overwriting hash tables, will be sufficient to qualify as 'erasure'. In my preliminary view that is, on the face of it, too weak to satisfy what is intended and stipulated by Article 17 GDPR. If Article 17 seeks to provide only for 'putting data beyond use' it would, I feel, have said so. The people doing the drafting would surely have been aware of the established legal precedents/court orders on data records, and recording media, destruction (and proof/certification thereof), corporate, industry and professional standards as regards Record Retention and Destruction, and Statutes providing Requirements and Guidelines for Public Bodies as regards Citizens' Records Disposal. **[7]**

It seems to me that, in regard to the true implication of 'erasure', which is the wording actually chosen, the intention and meaning is something stringent and strong. If GDPR intends 'erasure' just to mean 'putting data beyond use', or even 'deletion', in the usual technical sense that these terms are used, and implemented, in electronics and computer data technology practice, it would have said so – GDPR was years in the drafting, with many highly-qualified legal and technical people involved, globally, in intensive discussions and reviews, before finalisation.

No, 'erasure' is the word carefully enacted in the GDPR; and 'erasing' has many quite clear synonyms in English: eradicating, obliterating, destroying, abolishing, removing, shredding, disposing of, wiping out, dissolving, doing away with, getting rid of... At the extreme, where digital data recorded on servers, or electronically held, copied, distributed and communicated in computer and communications media, systems and networks are concerned, 'erasing' could arguably mean, for true efficacy in practice, 'returning to a free molecular state' by way, for example, of 'burning, consuming in flames'.

In my view it follows that anyone implementing applications or systems using a blockchain, given the *foundational, inherent 'permanence and immutability' of its data records*, where such records may contain personally identifiable details of a 'data subject', will do so at risk of not being physically or verifiably able to comply with Article 17 GDPR, and thus potentially subject to the significant financial and other penalties available and arising thereunder.

Lest it is thought that there is going to be little likelihood of requests, whether to companies or organisations holding or processing systems and databases containing personally identifiable details of 'data subjects', or to the courts, for applicant data subjects to be 'forgotten', well, I suggest: think again. A few years back the possibility of widespread use of such requests may have seemed fanciful, but since the *Cambridge Analytica* allegations – that this data analytics firm used personal information harvested from more than fifty million Facebook profiles, *without the data subjects' permission*, to build a system that could target US voters with personalised political advertisements based on their psychological profile – anyone using social media, for example, is now well aware of the right not to have personal data used for purposes for which they were not originally, and freely, provided.

Indeed, even before the coming into force of GDPR, the English Courts have already upheld such a critical request:

> https://www.theguardian.com/technology/2018/apr/13/google-loses-right-to-be-forgotten-case
> *Google loses landmark 'right to be forgotten' case Jamie Grierson Ben Quinn Fri 13 Apr 2018*
> *Businessman wins legal action to force removal of search results about past conviction*
> *A businessman has won his legal action to remove search results about a criminal conviction in a landmark "right to be forgotten" case that could have wide-ranging repercussions. … the claimant … was convicted more than 10 years ago of conspiracy …*

Conclusions

In summary, I suspect that some of the potential future issues that ICT systems professionals and experts may well be asked to investigate and upon which to provide analyses, conclusions and opinions, in regard to trust in, legal and technical reliability of, and associated disputes over, blockchain-based systems applications, are likely to include:

Cryptocurrency ICOs/ITOs:

- Allegations of false or negligent representations in 'White Papers', Public Issue Documentation and Presentations, Websites.
- Failure to carry out due diligence as to project viability, systems and business integrity, quality standards, financial probity, implementation rigour.
- Consequential losses: investors losing money, businesses going bust, causality.

Blockchain:

- Operational systems failures: the blockchain itself may be reasonably robust and reliable, but all interface/interconnect systems still need to be specified, designed, coded, constructed, tested and commissioned to acceptable ICT industry and professional standards.
- Consequences: assessment of outages, denial, inaccuracy and unreliability of service, data transaction failures, errors or faults, data going missing, people losing money unable to conduct reliable business, smart contracts corrupted, distributed ledgers not capable of being trusted.
- Assessment and apportionment of causality, liability, and responsibility for damages, losses and compensation.

Blockchain and GDPR Article 17:

- In regard to requests 'to be forgotten' by data subjects, where their personally identifiable data are held on 'permanent and immutable' blockchain records: advice and management of implementation of Court Orders granted for 'erasure'.
- Opinion as to efficacy of 'erasure' techniques, transactions, technologies, processes, proposed or implemented.
- Verification of the 'erasure' carried out: what constitutes sufficient evidence and proof of accuracy, correctness, completeness and persistence?
- Assistance with discussions with Information Commissioner's Office as to validity of requests 'to be forgotten', confirmation of the extent, reliability and security of 'erasure' (to be) carried out, and reasonableness of any possible/proposed fines or penalties to be imposed.

Ownership of IP:

- Advice and guidance as to: whether relying on third-party blockchain platforms, or developing its own blockchain software in-house, any developer or company seeking to build blockchain-based applications runs the risk of IP infringement (there are as yet no ISO standards, and already more than 650 blockchain patent applications filed with the US Patent Office).
- Assessment of impact, consequences, remediation: e.g. litigation over patents and software copyright.
- Expert investigation, search and advice as regards Prior Art, and/or Lack of Inventive Step, for patent infringement actions and challenges to the original Grant of Patent.
- Advice and guidance in connection with negotiations with patent or copyright owners over use restrictions, licence fees, development capability.

Clearly, future blockchain disputes and litigation could be an active area for ICT experts.

And Further…

This is of course in addition to the 'usual' relentless occurrence of disputes over computer systems failures generally. Failures of confidence, good faith and expectation (*Cambridge Analytica* alleged private data misuse), of dependable cybersecurity (potential *Facebook* password hacking), of mission-critical financial systems implementation (*TSB* online banking deficient systems upgrade), of product 'fitness for purpose' (*VW Dieselgate* emissions 'cheat' software), and of clinical operational reliability (*NHS* faulty breast cancer-screening algorithm): these are just a few examples of the latest crop in a steady and growing stream of ever-upscaling IT Disasters that have regularly emerged over the past thirty years.

I myself have been involved as expert witness in the largest and longest computer software and systems contractual disputes to date reaching the English High Court, and Sydney Supreme Court, with damages claimed in such actions in the hundreds of millions of pounds. Indeed, nearly twenty years ago, in the USA *Foxmeyer* case, we have already seen the failure of an entire substantial multi-billion corporation due to the faulty implementation and management of a major company-wide computer systems upgrade project **[8]**.

With *Blockchain*/*Distributed Ledger*/*Smart Contract*/*Cryptocurrency* developments and systems, and, we can reliably add, those now offering or dependent on *Visual/Augmented/Mixed Reality*/*Immersive Technology*, *The Internet of Things*/*Smart Buildings*/*The Connected Home*, *Data Analytics*/*GDPR*, and *Artificial Intelligence* (AI)/*Machine Learning*/*Algorithms*, disputes and damages over and/or caused by evermore-'intelligent' computer software and data communications and processing are certain to increase, and potentially cause increasingly widespread and relentlessly-larger financial and other anxiety, consequences and damages.

AI, Machine Learning and Robotics

In particular AI, robot systems, intelligent and autonomous devices (such as automobiles), assistive technologies, cyborgs and the like are set to make a huge impact on organisations, companies, societies and humanity as a whole in the coming years. I have urged the UK Prime Minister to give priority attention to this most important of existential challenges around right now: the Coming of the Robots. The Artificial Intelligence Age is well upon us, and the criticality of the issues raised by supra-smart, self-learning, űber-capable, interconnected software and technology devices and systems in my view vastly transcends anything else (trumping even Brexit).

In the early disruptive days of microcomputers, my call for an Action Group on Information Technology, *AGIT*, was widely published. This contributed to the extensive industry pleas for UK government action from the computer software and electronics community, and eventually saw Kenneth Baker appointed as Minister for IT, securing something of a UK position in the PC and Internet Age. I have similarly now proposed an Action Group on Robot Integration and Control, *AGRIC*, and have called on the UK PM to appoint a Senior Government *Minister for AI* to address the fundamentally new societal and regulatory challenges, and, equally, seize for the UK the new opportunities, arising from this rapidly evolving Machine Species.

The late Ian McNaught-Davis, ebullient presenter of BBC TV series such as *Micro Live* back in the 1980s, memorably said "*Never forget that the opposite of Artificial Intelligence is Real Stupidity*". AGRIC is intended actively to address that we are in imminent danger of being made to look really stupid by the robots.

AI vs Trust: oho yes, that is a topic for another whole article. Ethical algorithms? I don't think so. Trust me, I am an expert.

----- ooo END ooo -----

* Dr Stephen Castell CITP MIoD MEWI is Chairman of CASTELL Consulting, and is an award-winning independent ICT expert, management consultant and project manager professional, with extensive experience in risk assessment, quality assurance, and dispute resolution. He has for over twenty-five years acted internationally as an expert witness in major complex computer software and systems disputes and litigation, including the largest and longest such actions to have reached the English High Court (*AirTours v EDS*, 2001; *GEC-Marconi v LFCDA*, 1992) and Sydney Supreme Court (*ITSL & ERG v PTTC*, 2012), and in US IP (patent, software copyright, commercial secrets), data forensics, e-document authentication and software and technology valuation and quantum cases. His paper '*Forensic Systems Analysis: A Methodology for Assessment and Avoidance of IT Disasters and Disputes*' was issued as a *Cutter Consortium Executive Report*, Enterprise Risk Management & Governance Advisory Service series (Vol. 3, No. 2, March 8, 2006).
stephen@castellconsulting.com
http://www.castellconsulting.com/ http://www.e-expertwitness.com/

In the early 1980s he was a pioneer of the Over The Counter Market in the UK, raising risk capital for new technology-based companies, responsible for assessing several hundred such companies in a five year period, in preparing their flotation prospectuses, and serving as Non-Executive Director. In 1982, he was founder Technical Director of the venture capital funded *International Communications Technology Holdings SA*, based in Luxembourg and listed on the London Stock Exchange, and was Chairman of its UK subsidiary *Telephone Broadcasting Systems plc*.

He is a Panellist on CBTV ('CryptoBlockTV'), a blockchain and cryptocurrency programme on *Property TV*, broadcast in the UK on Sky198 (http://property-tv.co.uk/), and potentially appearing on, for example, Bloomberg TV and elsewhere. The initial poster programme is at: *https://vimeo.com/user36208838/review/257927211/7ff86eed15*

Dr Castell is the author of the best-selling *Computer Bluff* (1983, Quartermaine House, ISBN 0 905898 15 X), "The *Which Computer* book for people who know nothing about computers … and would like to have left it that way"; and of *The APPEAL Report* (1990, May, Eclipse Publications, ISBN 1-870771-03-6), a major study commissioned by the CCTA (H M Treasury) on the admissibility of computer evidence in court and the legal reliability/security of IT systems, still seen by many as a definitive study in the field. This concluded with what became known as:

> *Castell's (First) Dictum*: "*You cannot secure an ontologically unreliable technology by use of an ontologically unreliable technology*".

Electronic Evidence has since become widely acknowledged to be based on the concept of a transactional *chain of trust*, the latter's dependency on *Trusted Third Party Services* ('TTPs') being identified in 1993:

> "As described by Castell, '*A Trusted Third Party is an impartial organization delivering business confidence, through commercial and technical security features, to an electronic transaction. It supplies technically and legally reliable means of carrying out, facilitating, producing independent evidence about and/or arbitrating on an electronic transaction. Its services are provided and underwritten by technical, legal, financial and/or structural means*' [10]. TTPs are provided and underwritten not only by technical, but also by legal, financial, and structural means [10,11]. TTPs are operationally connected through chains of trust (usually called certificate paths) in order to provide a web of trust…
>
> [10] S. Castell, Code of practice and management guidelines for trusted third party services, INFOSEC Project Report S2101/02, 1993.
>
> [11] Commission of the European Community. Green paper on the security of information systems, ver. 4.2.1, 1994. …"

In *Security Issues On Cloud Computing.* Pratibha Tripathi, Mohammad Suaib;
Department of Computer Science and Engineering, Integral University, Lucknow, Uttar Pradesh, India.
International Journal of Engineering Technology, Management and Applied Sciences
http://www.ijetmas.com/ November2014, Volume 2 Issue 6, ISSN 2349-44761.
Available from: https://www.researchgate.net/publication/272945014_Security_Issues_On_Cloud_Computing

A ***Draft Convention on Electronic Evidence*** has recently been published as a supplement to the **Volume 13: 2016** issue of the **Digital Evidence and Electronic Signature Law Review**. It is authored by **Stephen Mason** (http://www.stephenmason.eu/), a barrister of the Middle Temple and a recognised authority on electronic signatures and digital evidence. To obtain and review the ***Draft Convention on Electronic Evidence***:

1. Go to http://journals.sas.ac.uk/deeslr/issue/view/336/showToc
2. See 'Documents Supplement' at foot of contents; click on 'Draft Convention on Electronic Evidence' to see Abstract: http://dx.doi.org/10.14296/deeslr.v13i0.2321
3. Then click on 'PDF' (http://journals.sas.ac.uk/deeslr/article/view/2321/2245) to download the full text of the Draft Convention.

** https://theregaconference.com/

> *Since its enactment in 2015, Regulation A has offered an exemption from registration requirements for smaller companies that want to raise equity capital through a public offering of securities. Instituted by the Securities Act, Regulation A creates two tiers of public offerings. Each comes with distinctly different reporting and disclosure requirements as well as separate ceilings for the value of securities that can be issued in any given year. The Reg A Conference dives into these topics with a slate of experts who know the rules of the road when it comes to securities offerings. Hear from executives who've steered their companies through public offerings, as well as legal experts, accountants, and investment bankers who help ensure optimal results. Learn about the distinct format options for preparing a prospectus, as well as what to include.*

https://www.investopedia.com/terms/r/regulationa.asp

> *Regulation A is an exemption from registration requirements – instituted by the Securities Act – that apply to public offerings of securities that do not exceed $5 million in any one-year period. Companies utilizing the Regulation A exemption must still file offering statements with the Securities and Exchange Commission (SEC). However, the companies utilizing the exemption are given distinct advantages over companies that must fully register. The issuer of a Regulation A offering must give buyers documentation with the issue, similar to the prospectus of a registered offering. …*

Notes and References

[1] https://hackernoon.com/forever-on-the-chain-c755838dfc79
Júlio Santos, November 14, 2017. CTO at Fractal Blockchain. Decentralization, Censorship Resistance and Open Source. https://lifeonmars.pt

[2] A small selection on Initial Coin Offerings etc
https://flagtheory.com/successful-initial-coin-offering/
https://flagtheory.com/set-up-company-initial-coin-offering/
https://bitcoinmagazine.com/articles/sec-chairs-written-testimony-hints-moderation-cryptocurrencies-icos-be-warned/
https://www.coindesk.com/sec-compliance-office-step-crypto-disclosure-policing/
https://www.coindesk.com/marco-santori-dean-blockchain-lawyers-just-got-new-job/
https://www.banking.senate.gov/hearings/virtual-currencies-the-oversight-role-of-the-us-securities-and-exchange-commission-and-the-us-commodity-futures-trading-commission

And see '*Revolution of securities law in the Internet Age: A review on equity crowd-funding*', Tao Huang and Yuan Zhao, *Computer Law & Security Review*, 33, (2017) 802-810.

[3] '*What the ECU stands for*', Stephen Castell, Letter in *Computing*, 20 July 1995.
'*Ye Nom De Das Geld*', Stephen Castell, *GONG* Magazine, December 1971, pp16-18.

[4] Blockchain Standards
https://www.iso.org/committee/6266604.html
Creation date: 2016 ISO/TC 307 Blockchain and distributed ledger technologies
Scope: Standardisation of blockchain technologies and distributed ledger technologies.
8 ISO standards under development under the direct responsibility of ISO/TC 307
34 Participating members 12 Observing members

The Law Society HORIZON SCANNING August 2017, 12 pages: '*Blockchain – The Legal Implications of Distributed Systems*'.

Blockchain Patents
https://worldwide.espacenet.com/searchResults?ST=singleline&locale=en_EP&submitted=true&DB=&query=blockchainhttps://clarivate.com/blog/overview-blockchain-patent-landscape/.
https://clarivate.com/blog/overview-blockchain-patent-landscape/
These 650 (approximately) 'blockchain' patents – though perhaps not yet all granted, let alone challenged – may illustrate a difficulty that the ISO Working Parties could encounter in trying to define 'International Standards', essentially meant to be 'Open Source'.

https://www.infosys.com/Oracle/white-papers/Documents/integrating-blockchain-erp.pdf
http://www.primechaintech.com/assets/docs/PT-BSC-0_4.pdf
Primechain Technologies Blockchain Security Controls Version 0.4 dated 21st October, 2017
https://www.dlapiper.com/en/uk/insights/publications/2017/06/blockchain-background-challenges-legal-issues/
2 FEB 2018 Blockchain: background, challenges and legal issues
By:John McKinlay Duncan Pithouse John McGonagle Jessica Sanders (née Turner)
https://www.forbes.com/sites/laurashin/2016/05/10/looking-to-integrate-blockchain-into-your-business-heres-how/#4986f47f1a15
May 10, 2016 Looking To Integrate Blockchain Into Your Business? Here's How Laura Shin
Companies … are sprinting to begin adopting blockchain — the technology behind Bitcoin that promises to improve efficiency in numerous processes … But many are doing so simply because of fear of missing out, without a clear understanding of how it can be useful …

[5] https://www.prnewswire.com/news-releases/silver-miller-files-class-action-lawsuit-against-monkey-capital-and-its-principal-daniel-harrison-for-alleged-fraudulently-promoted-and-aborted-initial-coin-offering-300574019.html
… CORAL SPRINGS, Fla., Dec. 20, 2017 … www.SilverMillerLaw.com … actions currently pending against the Coinbase, Kraken, and Cryptsy exchanges as well as the first federally-filed class action lawsuit against heavily-embattled Tezos and its billion dollar … ICO … -- has filed a new federal court class action lawsuit against Monkey Capital and its principal, Daniel Harrison. … alleges, Monkey Capital fraudulently promoted an ICO that violated numerous state and federal securities laws. …
https://www.silvermillerlaw.com/david-silver/2017/12/20/silver-miller-files-class-action-lawsuit-monkey-capital-principal-daniel-harrison-fraudulently-promoted-aborted-initial-coin-offering/
… As ICOs have become more frequently used as a fundraising tool for start-up blockchain technology companies, so too has fraud upon cryptocurrency investors become more frequent; and Monkey Capital appears to have been a prime example of the harm investors can suffer … See the Class Action Complaint: Hodges, et al. v. Monkey Capital LLC, et al. …
https://www.silvermillerlaw.com/wp-content/uploads/2017/12/2017-12-19-DE-1-CLASS-ACTION-COMPLAINT.pdf

[6] 'CASTELL - Legal Due Diligence for Initial Coin Offering 07Feb2018.pdf'. Available privately from the author, on application.

[7] https://hackernoon.com/forever-on-the-chain-c755838dfc79
https://bitsonblocks.net/2016/02/29/a-gentle-introduction-to-immutability-of-blockchains/
https://www.coindesk.com/blockchain-immutability-myth/
https://www.forbes.com/sites/yec/2017/05/04/debunking-blockchain-myths-and-how-they-will-impact-the-future-of-business/#583e1d815609
https://www.records.nsw.gov.au/recordkeeping/advice/retention-and-disposal/destruction-of-records
https://ct.wolterskluwer.com/resource-center/articles/three-simple-rules-record-retention
http://apps.americanbar.org/buslaw/newsletter/0019/materials/recordretention.pdf
https://www.scality.com/blog/fuhgettaboutit-the-gdpr-right-to-erasure/

[8] https://www.slideshare.net/shaunaksontakke/batch-25-it-erp
ERP Case Study - Failure case - FoxMeyer Case Shaunak Sontakke … April 17, 2014
... FoxMeyer was the fifth largest drug wholesaler in the United States (1995) with annual sales of about 5 billion US$ and daily shipments of over 500,000 items. ... The company had 25 distribution centers located throughout USA. ... FoxMeyer was driven to bankruptcy in 1996, and the trustee of FoxMeyer announced in 1998 that he is suing SAP, the ERP vendor, as well as Andersen Consulting, its SAP integrator, for $500 million each ...

http://calleam.com/WTPF/?p=3508
Fox-Meyer Drugs A $65M investment in an Enterprise Resource Planning System (ERP) and new warehousing facilities results in the destruction of a $40B business. … Delays in delivery and the failure to fully realize the business benefits results in the organization being unable to profitably service contracts it had entered into. … When the system was delayed and when it failed to meet performance requirements … cash flow issues forced the company into Chapter 11 bankruptcy. The company that had been worth $40B prior to the project was then sold off for just $80M to rival McKesson Corp ...

Dr Stephen Castell CITP CPhys FIMA MEWI MIoD,
Chairman, CASTELL Consulting
PO Box 334,
Witham,
Essex CM8 3LP, UK
Tel: +44 1621 891 776   Mob: +44 7831 349 162
Email: stephen@castellconsulting.com
http://www.CastellConsulting.com
http://www.e-expertwitness.com

[5,600 words approximately]