Blockchain vs Trust: The Fundamental Expert Dilemma

by Dr Stephen Castell

Abstract:
The General Data Protection Regulation (GDPR) includes in its provisions Article 17, the Right to be Forgotten, which could potentially be a formidable barrier to the ubiquitous introduction of cryptographic blockchain software and technology. Despite this, there has been an investment mania for Blockchain Technology, with more money having gone into Bitcoin and other cryptocurrencies, blockchain, smart contracts and distributed ledger technology than even into Artificial Intelligence (AI). A few of these may prove to be commercially-successful, disruptive game-changers, and usher in the possibility of a new global 'crypto-economy' paradigm. But so far many have tended to have been significantly fuelled by the 'black cash' of drug-dealers, money-launders, traffickers and the like; and in Q2 2019, misappropriation of cryptocurrency funds netted criminals some $4.26 billion. The foundations of global digital currencies go back well before the Satoshi bitcoin paper of 2008. Those early digital e-commerce visions did not require a cryptographic blockchain 'mining', or 'distributed consensus', existential model, and were not intentioned of being so readily riven with the criminal black market profiteering of money-launders, scammers and fraudsters that bedevil much current cryptocurrency activity. Looking ahead, Facebook's Libra digital currency could establish a new global e-commerce paradigm much closer to the pre-bitcoin electronic cash visions, and one more compliant with the existing norms and customs of the Rule of Law, where a responsible Trusted Third Party, in this case, Facebook, is fundamental. Cryptocurrencies apart, some blockchain applications more generally are likely here to stay, and the majority will be robust implementations by established major corporations, with most of us, as consumers, hardly needing to know any of the details. For the properly-cautious ICT expert and professional, when considering the use of blockchain for any proposed use case, the 'fundamental things apply'. The legal status of blockchain cryptocurrency, smart contract and distributed ledger technology is not clear, or uncontentious, and in the USA, there is already ICO litigation on foot. There is always the need for Trusted Third Parties, and for probative Electronic Evidence. Crypto Dragons, the many and varied Financial Disputes over Crypto Assets have arrived. Such complaints, disagreements, conflicts, with civil and criminal claims and legal actions, are increasing, driven by the growth in crypto scams, thefts, losses and investigations,

with many such disputes reaching the courts. A key point at trial will be examination of the Digital Evidence and, although a Crypto Asset may essentially be 'decentralized digital vapour', a Court of Law can make a binding Order to get forensic traction on it, because of the legally well-established Obligation of Disclosure. This article concludes with a Checklist giving practical, generally applicable wording for an effective Digital Asset Disclosure exercise.

1. Introduction:
Blockchain and the Right to be Forgotten

"Blockchain technology introduces permanence and immutability into the digital world. … the technological revolution that commoditizes trust … Trust normally has to be enforced via laws, courts, … 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. …"
Júlio Santos, November 6th, 2017 [1].

The Right to be Forgotten could potentially be a formidable 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; …*

With the 'permanence and immutability' of data records written to the blockchain being emphasised as one of its fundamental, key features, in a wide range of use cases where acquisition, processing and recording of personal data is critical blockchain could possibly be structurally unable to be compliant with Article 17, Right to Erasure, of GDPR. The Commission nationale de l'informatique et des libertés (CNIL), the independent French administrative regulatory body whose mission is to ensure that data privacy law is applied to the collection, storage, and use of personal data, has identified this fundamental issue:

"… one of the characteristics of blockchains is that the data registered on a blockchain cannot be technically altered or deleted: once a block in which a transaction is recorded has been accepted by the majority of the participants, that transaction can no longer be altered in practice. … technical solutions … should be examined by stakeholders in order to solve this issue. The CNIL … questions their ability to ensure a full compliance with the GDPR. …

As a reminder, a blockchain can contain two categories of personal data:

The identifiers of participants and miners:

Each participant has an identifier comprised of a series of alphanumeric characters which look random, and which constitute the public key to the participant's account. This public key is linked to a private key, known only by the participant…

The CNIL therefore considers that this data cannot be further minimised and that their retention periods are, by essence, in line with the blockchain's duration of existence.
Additional data (or payload):

Besides the participants' identifiers, the additional data stored on the blockchain can contain personal data, which can potentially relate to individuals other than participants and miners.

As a reminder, the principle of data protection by design (Art 25 of GDPR) requires the data controller to choose the format with the least impact on individuals' rights and freedoms."

Others have proposed potential technical solutions, for example:
"The Workaround …Storing personal data on a blockchain is not an option anymore according to GDPR. A popular option to get around this problem is a very simple one: You store the personal data ***off-chain*** *and store the reference to this data, along with a hash of this data and other metadata (like claims and permissions about this data),* ***on*** *the blockchain."*
Andries Van Humbeeck, November 21, 2017 [2].

There is also a technician's view that, in regard to interpreting and implementing 'erasure' in practice, simply 'putting data beyond use' electronically will satisfy 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'.

However, I consider this too weak to satisfy what is intended and stipulated by Article 17 GDPR. If Article 17 had sought to provide only for 'putting data beyond use' it would have said so. The people doing the drafting would have been aware of, amongst other things, the established legal precedents and 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 [3].

The word chosen in Article 17 of GDPR is 'erasure', and its intention and meaning is something clear, stringent and strong. If GDPR had intended 'erasure' just to mean, or include, '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 made that, too, clear.

GDPR was years in the drafting, with many highly-qualified legal and technical people involved, globally, in intensive discussions and reviews, before finalisation. 'Erasure' and 'erased', being the actual words carefully enacted in the GDPR, have many clear synonyms in English: 'Erasing': eradicating, obliterating, destroying, abolishing, removing, shredding, disposing of, wiping out, dissolving, doing away with, getting rid of...

From an expert point of view, where digital data recorded on servers, or electronically held, copied, distributed and communicated in computer and communications media, systems and networks are concerned, 'erasing' can even mean, for true efficacy in practice, 'returning to a free molecular state' by way, for example, of 'burning, consuming in flames'.

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.

It may be considered that there will 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'. 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.

Furthermore, even before the coming into force of GDPR the English Courts had upheld such a critical request: 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 … [4].

2. The new 'crypto-economy' - a fraudsters' playground?

Despite that the GDPR Article 17 risk to systems implemented using a blockchain, in use cases where personal data is to be recorded, presents a potentially serious implementation difficulty, there has been an investment mania for Crypto-Algorithmic Blockchain Technology, with far more money having gone into - gambled on - Bitcoin and other cryptocurrencies, blockchain, smart contracts and distributed ledger technology than even into Artificial Intelligence (AI). It has in the past seemed that almost every other Millennial was 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' raised billions in real legal tender, 'fiat currencies'.

This substantial finance-raising has been used to fund fantasy coins and tokens, with no obvious economic utility or asset value, 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'. A few of these may prove to be commercially-successful, reputable, significantly disruptive game-changers, and usher in the possibility of a new global 'crypto-economy' paradigm. But so far, it has often been discovered that ICOs/ITOs, cryptocurrency 'mining', and crypto-coin trading exchanges have tended to have been significantly fuelled or taken over by the 'black cash' of drug-dealers, money-launders, traffickers and the like, and in a substantive not-easily-reversible way.

The 'Q2 2019 Cryptocurrency Anti-Money Laundering Report' from Ciphertrace revealed that misappropriation of funds "from cryptocurrency users and exchanges netted criminals and fraudsters approximately $4.26 billion in aggregate". This is in the context of the amount of cryptocurrency traded in September 2019 on crypto-trading exchanges being over $500 billion (down from nearly $800 billion in June 2019), with Hong Kong-based exchange Binance reporting that, in the last two years, it alone made over $1billion of profit.

Many of those yearning for the putative 'crypto-economy', for example Millennials let down after the post-2008 credit crunch by governments, the banks, and educational system, have tended to disregard any need to be subject to Know Your Client (KYC) and Anti-Money Laundering (AML) strictures, and may not have been too worried from whence came their ICO money, how it was actually going to be (accountably) spent, or whether it could even possibly result in a viable business.

It is worth being reminded that the foundations of global digital currencies go back well before the Satoshi bitcoin paper of 2008. The early pioneering international digital economy e-commerce visions did not require a cryptographic blockchain 'mining', or 'distributed consensus', existential model. And they certainly were not intentioned by any thought or expectation of becoming so readily riven with the criminal black market profiteering of money-launders, scammers and fraudsters that apparently increasingly bedevil much - but of course not all - current cryptocurrency activity.

David Chaum, in a scientific paper of 1983, is reckoned to be the first to describe digital money. His proposal used cryptography to create a blind, digital signature to make money anonymous, and he founded a company in 1989 that invented the virtual currency DigiCash. -But it had a hard time commercially, with a 1999 article in Forbes summing it up as: "A beautiful idea for a beautiful new world with one problem: nobody wants it. Not the banks, not the dealers and above all, not the customers. E-commerce is flourishing, but as it turns out, the customer's Mastercard and Visa are his preferred currencies".

Milton Friedman, the economist, said in 1999: "One thing we are still lacking and will soon develop is reliable e-cash- a method by which money can be transferred from A to B on the Internet without A knowing B and vice versa". Even earlier than these, I myself put forward, nearly thirty-five

years ago, a new, disintermediated wholly digital cash currency, as set out in my 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. … the Electronic Cash Unit".

And, long before Millennials were even born, my fictional article, 'Ye Nom De Das Geld', in the December 1971 issue of GONG (the student magazine of the University of Nottingham), went even further with my vision 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. … ".

Looking ahead, Facebook has plans for its Libra digital currency that so worry regulators they are seriously considering trying to prevent it happening; but it may already be too late, and Libra could be 'unstoppable'. Facebook recently reported that it now has 2.4bn monthly users across its various apps with users on at least one of these apps every day. Furthermore, Libra may turn out to have little to do with any putative 'crypto-economy' and could establish a powerful new digitalised global e-commerce paradigm much closer to the pre-bitcoin electronic cash visions of early digital currency thought-leaders and entrepreneurs – and a paradigm more comfortably compliant with the existing human society and regulatory norms and customs of the Rule of Law, where a responsible Trusted Third Party, in this case, Facebook, is fundamental, and pivotal.

For all these reasons many of the current species of cryptocurrencies - not excluding Bitcoin - may in their present manifestations fade away, and/or the hoped-for 'crypto-economy' may at some point even be regulated out of existence [5].

3. Blockchain: Sceptical ICT Professionalism and Legal Due Diligence

Cryptocurrencies apart, however, some blockchain applications more generally are likely 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, a widespread settled, but vigorous and continually innovating, 'blockchain applications industry' may be in place, one perhaps bearing little resemblance to the frantic cryptocurrency 'bandit territory' landscape of today.

For the properly-cautious ICT expert and professional, when considering the use of blockchain for any proposed use case, the 'fundamental things apply'. This caution is an essential 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, that not only are there no finalised international/ISO standards yet for blockchain (the eight standards in development under ISO/TC 307 are not due out until 2020 at the earliest), but also there is far more to specifying, designing, developing, testing, deploying and maintaining an appropriate complete QA-assured system than just 'the blockchain component'.

And whether to use blockchain as a component at all for a given business/system requirement is a critical feasibility exercise that the seasoned professional will know is vital. Any duly diligent ICT systems engineer may therefore 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. Ideally this will also take properly risk-assessed competitive advantage of any – and not just crypto, or blockchain – new developments in technologies, tools, methodologies and processes, always consistent with the budget/price willing to be paid, of course [6].

Furthermore, the legal status of blockchain cryptocurrency, smart contract and distributed ledger technology is not clear, or uncontentious. In the USA, there is already ICO litigation on foot [7]. Having been involved in advising on ICOs, 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 proficient, high-profile, software engineering entrepreneur and thought-leader, let us call him Joshua, a US citizen, a highly experienced and imaginative technical and regulatory expert working in the blockchain and cryptocurrencies field, is 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". 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 equivalent to issuing a security, would it not be advisable 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 trade-

mark 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 made misrepresentations, and was negligent/fraudulent, and thus seek reparations or, worse, criminal prosecution, what can he 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 he can take? [8].

4. The need for Trusted Third Parties, and for probative Electronic Evidence

Commissioned by the UK's CCTA (H M Treasury), I carried out a major study, still seen by many as definitive in the field, on the admissibility of computer evidence in court and the legal reliability/security of IT systems, published as The APPEAL Report (1990). 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".

It is vital for any operational computer system, and, not least, one purporting to provide goods, services, currencies, communications etc to the public, upon which the public relies, to have one or more Trusted Third Party (TTP) standing behind it and responsible for it, given the ontological unreliability of computer technology, and the associated need for disclosure of probative Electronic Evidence and computer 'documents' when (not if!) disputes arise. Electronic Evidence has become widely acknowledged to be based on the concept of a transactional chain of trust, and I also identified in 1993 the latter's dependency on Trusted Third Party Services (TTPS):
"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".

Thus TTPS are provided and underwritten not only by technical, but also by legal, financial, and structural means and are operationally connected through chains of trust (usually called certificate paths) in order to provide a web of trust: the whole structure being what we might call simply an Implementation of the Rule of Law [9].

5. Conclusions: Blockchain vs. Trust - the Future Expert Issues in Disputes over Crypto Assets

Given that it is implicit that the trust and reliability of 'blockchain only' systems and services are provided merely technically, by virtue of the 'distributed consensus' algorithm, there is essentially and fundamentally no TTP involved or standing behind the creation and valuation of, and dealing and trading in, blockchain-held Crypto Assets. The internet is not a sue-able party. It has no intrinsic financial value, and 'belongs' to no-one. Since a Crypto Asset fundamentally consists of zeros and ones scratched on an internet-accessed blockchain, changes stored and processed, written into, a distributed ledger, it may seem futile, perhaps legally meaningless, to ascribe a tangible value to a decentralized blockchain, without any substantive, sue-able TTP responsible for or standing behind its integrity and security.

However, when Crypto Assets become the subject of disputes - Crypto Dragons, as I christened them, in a recent article in Solicitors Journal - the identification, location, and financial valuation of any Crypto Asset, access to it, holdings of it, and dealings and trading in it, will be critical.

And here's the key point: Crypto Asset holdings and dealings are certainly not beyond legal protection or action, nor regulatory reach. Although a Crypto Asset may essentially be 'decentralized digital vapour' a Court of Law can make a binding Order to get forensic traction on it, because of the legally well-established Obligation of Disclosure. This obligation applies as much to a digital Crypto Asset as it does routinely to all other computer-held digital materials and 'documents', i.e. the Electronic Evidence relevant to any forensic investigation, whether for a Civil Dispute or for a Criminal Prosecution.

Thus, Disclosure and Valuation of Digital Assets, including Crypto Assets, is a significant issue arising in such financial and technology legal actions, Civil or Criminal. During years of expert witness work I have routinely assisted solicitors and Senior Counsel in framing appropriate technical Requests for Disclosure, and at request of attorneys I recently drafted a Checklist giving practical, generally applicable wording for an effective Digital Asset Disclosure exercise. Details of my Digital Asset Disclosure Wording Checklist are summarised in my October 2019 article in Solicitors Journal [10].

The Checklist should assist litigation lawyers and ICT experts, in Financial Audit, Tax Assessment, Fraud and Theft Enquiry, Fintech Due Diligence, Investment Exchange Issues and Listings, M&A Projects, Corporate Risk Assessments, Divorce Proceedings, IP Conflicts and Smart Contract Audit forensic investigations.

More generally, 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, business 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 quality assurance 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, or linked to, 'permanent and immutable' blockchain records: advice and management in regard to 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, any company seeking to build blockchain-based applications runs an IP infringement risk (there are no ISO standards, and more than 1,000 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.

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), of clinical operational reliability (NHS faulty breast cancer-screening algorithm), and of aircraft flight systems reliability and integrity (Boeing 737 MAX crashes): these are just a few examples of a growing stream of ever-upscaling IT Disasters that have regularly emerged over the past thirty years.

I 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, the failure of an entire substantial multi-billion corporation occurred and was directly due to the faulty implementation and management of a major company-wide computer systems upgrade project [11].

With blockchain-based Distributed Ledger, Smart Contract and Cryptocurrency developments and systems becoming ever more established, Crypto Dragon disputes - whether Civil, or Criminal (thefts, scams, frauds) - are certain to increase, and potentially cause increasingly widespread and relentlessly-larger financial and other anxiety, consequences and damages. When it is your Crypto Assets that are the ones under examination in pursuit of, or arising from, disputes, allegations, valuations, tax demands, thefts, systems failures, prosecutions or other forensic investigations you had better hope that there is a TTP to be held responsible for disclosing the Electronic Evidence essential to your case, rather than rely on the 'trustless' digital cipher of the blockchain 'distributed consensus' mechanism itself to be of any practical or material human assistance.

Biographical Note

Dr Stephen Castell CITP CPhys FIMA MEWI MIoD, Chairman of CASTELL Consulting, is an award-winning independent ICT expert, management consultant and project manager professional, with extensive experience in risk assessment, quality assurance, and dispute resolution. For over thirty years Dr Castell has 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 IP (patent, software copyright, commercial secrets actions, eg USA cases BI v Echostar and Lodsys v Kaspersky), data forensics, e-document authentication and software and technology valuation and quantum cases. His seminal paper 'Forensic Systems Analysis: A Methodology for Assessment and Avoidance of IT Disasters and Disputes' is a Cutter Consortium Executive Report, Enterprise Risk Management & Governance Advisory Service series (Vol. 3, No. 2, March 8, 2006).

In the early 1980s Dr Castell was a high-profile 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. The initial poster programme is at: www.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".

References

1. 'Forever on the Chain' https://hackernoon.com/forever-on-the-chain-c755838dfc79
Júlio Santos, November 6th, 2017. https://lifeonmars.pt

2. 'Solutions for a responsible use of the blockchain in the context of personal data'
https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf

'The Blockchain-GDPR Paradox'
https://medium.com/wearetheledger/the-blockchain-gdpr-paradox-fc51e663d047

Andries Van Humbeeck, November 21, 2017.
https://theledger.be/

3. 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

https://www.proshred.com/documentation-retention-policies-potential-ramifications/

http://www.pbi.org/docs/default-source/default-document-library/10778_minimizing-commercial-litigation-risks-(2019).pdf?sfvrsn=0

"Minimizing Commercial Litigation Risks … 9. Implement a Document Retention Policy…".
https://www.scality.com/blog/fuhgettaboutit-the-gdpr-right-to-erasure/

4. https://internetofbusiness.com/solid-pods-how-sir-tim-berners-lee-aims-to-inrupt-the-web-from-within/
The position, security, ownership, handling, (mis)use, etc of 'personal data' and who should profit from such data, is becoming central to the future social media and digital economy, globally. Sir Tim Berners-Lee has introduced a new breed of " … personal online data stores, or Pods, that contain the wealth of information people generate, and are their exclusive property …", as part of the future 'Web 3.0'.

My own www.Zykme.net, a new P2P cross-platform comms App (hybrid, beta test version), designed to provide instant private one-to-one secure transfer of personal data using a unique proprietary one-time Zykword code protocol, is consistent with this Pod Philosophy. The Zykme App does not demand the user's email address, nor any other 'logon' ID data; and, as made clear at the foot of its 'Your ZykPod History of Contacts Received" page, "NOTE Unlike other social media, this unique Zykme App, which securely provides instant two-way peer-to-peer communication, does not and will not acquire, store, process, analyse, use nor pass on to any third party any of your entered data. Using Zykme, your personal 'My details' information as 'Sender' remains completely under your control, and, at entirely your own decision and choice, is privately and confidentially shared and exchanged between you and your selected 'Receiver' alone, when you press 'Share info'".

5. '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.

https://www.arachnys.com/2019/10/22/addressing-the-aml-risks-of-cryptocurrencies/

"Addressing the AML risks of cryptocurrencies OCTOBER 22, 2019 BLOG
With the recent explosion in cryptocurrencies, from the early beginnings of Bitcoin back in 2009 through to J.P. Morgan testing their own digital coins for institutional clients in 2019, there still remains serious unanswered questions about the money laundering risks they bring to banks, consumers and regulators. Ciphertrace's 'Q2 2019 Cryptocurrency Anti-Money Laundering Report' makes some stark revelations. It claims that theft, scams and other forms of misappropriation of funds "from cryptocurrency users and exchanges netted criminals and fraudsters approximately $4.26 billion in aggregate. … Dr Stephen Castell, an independent FinTech consultant, admits that there are few innocent investor protections to fall back on: "This is essentially the case worldwide today, and it looks like it will continue that way for the foreseeable future." He reminds us that there is a need to keep everything in perspective, suggesting that "the actual, and potential, total global 'crypto' business for banks and other financial institutions is tiny – in the less than 1% area." So, with the increased anti-money laundering (AML) risks associated with blockchains and cryptocurrencies, he believes it's right for the compliance departments of banks to proceed cautiously, if at all. …".

"… Traditional exchanges around the world will be looking at Binance's latest quarterly results with envy, as in the last two years it has made over $1billion of profit. CEO of Binance, Changpeng Zhao, sometimes called CZ (Chinese-born, now living in Vancouver) established Binance only in 2017. Binance raised $15 million via an Initial Coin Offering (ICO) and CZ is reported to be worth $1.2 billion. Binance, based in Hong Kong, is different from its competitors which, apart from Huobi (Singapore), are based in the USA e.g. Coinbase (San Fran), Kraken (San Fran), Bittex (Las Vagas) and Bitbox (NYC). The amount of Cryptos that were traded in September 2019 on exchanges like Binance was still over $500 billion - down from nearly $800 billion in June 2019. According to the website Coin.Market there are now over 260 different Crypto exchanges …".

Digital Bytes, Weekending 26th October 2019, Team-Blockchain Ltd.
http://www.teamblockchain.net/

https://hackernoon.com/the-amazing-story-of-cryptocurrencies-before-bitcoin-fe1b0e55155b

"The Amazing Story of Cryptocurrencies Before Bitcoin Marcell Nimfuehr, October 14th 2019

What—you exclaim with disbelief. Cryptocurrencies before Bitcoin? Yes, indeed. Don't get me wrong, Bitcoin was the first blockchain-based currency. But by far not the first purely digital money. That one has a colorful history of dreams, prosecution and failure. ...".

https://www.dcforecasts.com/libra-coin-news/chinese-crypto-czar-facebooks-libra-might-be-unstoppable/
"Chinese Crypto Czar: Facebook's Libra 'Might Be Unstoppable' September 20, 2019 By Stefan".

6. Blockchain Standards
https://www.iso.org/committee/6266604.html
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

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

Blockchain Patents
https://worldwide.espacenet.com/searchResults?ST=single-line&locale=en_EP&submitted=true&DB=&query=blockchain

https://www.cnbc.com/2019/03/25/bank-of-america-skeptical-on-blockchain-despite-having-most-patents.html

https://www.americanbar.org/groups/intellectual_property_law/publications/landslide/2017-18/march-april/patentability-blockchain-technology-future-innovation/

https://thenextweb.com/hardfork/2019/03/13/data-china-is-patenting-all-the-blockchain-tech-despite-banning-cryptocurrency/

The many 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', which are 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 …"

7. 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 … 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

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

9. The APPEAL Report, Dr Stephen Castell, 1990, May, Eclipse Publications, ISBN 1-870771-03-6).

'Code of practice and management guidelines for trusted third party services', S. Castell, INFOSEC Project Report S2101/02, 1993.

'Green paper on the security of information systems', Commission of the European Community, ver. 4.2.1, 1994.

See also 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/ November 2014, Volume 2 Issue 6, ISSN 2349-44761. Available from: https://www.researchgate.net/publication/272945014_Security_Issues_On_Cloud_Computing

The Draft Convention on Electronic Evidence has recently been published, in 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, with contributions by Dr Stephen Castell. 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.

10. 'Authored by AI - Here be crypto dragons: it's all about the evidence, proclaims the CastellGhostWriteBot', Stephen Castell, Solicitors Journal, October 2019, pages 43-45. https://www.solicitorsjournal.com/feature/201910/authored-ai

"Can you tell if this has been authored by a robot? Would it matter, legally or otherwise, if you couldn't? Are you crypto-friendly, or if not, at least crypto-aware? …".

And see:

'The future decisions of RoboJudge HHJ Arthur Ian Blockchain: Dread, delight or derision?', Castell, S. (2018), Computer Law & Security Review, Volume 34, Issue 4, August 2018, Pages 739-753, the Landmark 200th issue of CLSR under the Editorship of Emeritus Professor Steve Saxby. https://doi.org/10.1016/j.clsr.2018.05.011. While many are concerned about defining and developing AI Machine Ethics, Castell's Second Dictum: "You cannot construct an algorithm that will reliably decide whether or not any algorithm is ethical" (2017) reveals that this is a futile exercise. "Talking about the ethics of machines might be like speaking of the happiness of water" (page 743).

'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.

11. 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. ... 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. … 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 ...".

Correspondence:
CASTELL Consulting;
PO Box 334, Witham
Essex CM8 3LP
United Kingdom

Email: stephen@castellconsulting.com
Website: www.e-expertwitness.com
Alternate Website: www.CastellConsulting.com
Tel.: +44 7831 349 162
Mob: +44 7831 349 162