From: Dr Stephen CASTELL - France [mailto:0609961053@sfr.fr]
Sent: 20 August 2018 21:32
To: Friends and Colleagues <stephen@castellconsulting.com>
Subject: Blockchain & the USA November 2018 Elections: Expert Analysis of West Virginia's Blockchain-based Voting App

Please Reply direct to stephen@castellconsulting.com [and NOT to this email address 0609961053@sfr.fr]. Many thanks.

"West Virginia residents … will have the option of voting by smartphone in the November 2018 election … state officials have affirmed that the technology is secure".

Legal Technology Expert Nick Rishwain Interviews Computer Systems Expert Regarding Potential Election Hacking
https://www.robinettelaw.com/blog/2018/08/smartphone-voting-app-for-deployed-west-virginia-military.shtml
Smartphone Voting App for Deployed West Virginia Military By Terri Robinette of Robinette Legal Group, PLLC … Thursday, August 16, 2018.
… Election hacking in West Virginia is a longstanding tradition. … From stuffed votes to cold votes (votes from the deceased), election tampering has occurred on many levels. … Legal technology expert Nick Rishwain recently published an analysis of the West Virginia plan … Mr. Rishwain interviews ***Dr. Stephen Castell****, a computer science and systems expert witness with over 30 years of experience. As an expert witness, Dr. Castell has acted in over 100 major cases including the largest and longest computer software actions to have come to trial in the English High Court. …*

Computer Science and Systems Expert Witness – Dr. Stephen Castell
https://experts-blog.com/2018/08/14/blockchain-voting-election-2018-expert-analysis-of-west-virginias-plan/
Blockchain Voting Election 2018: Expert Analysis of West Virginia's Plan … Nick Rishwain on August 14, 2018 …
… I have a lot of questions about the security and reliability of the voting application offered by ***Voatz****. …*
Nick*: Is a Blockchain-based voting system secure?*
Dr. Castell*: The Blockchain in and of itself provides strong cryptographic security. However, ICT expert professionals bear in mind that not only are there no finalised international standards for Blockchain… but also there is far more to specifying, designing, developing, testing, deploying and maintaining an appropriate complete QA'd application than just the Blockchain element. The security of the complete system needs to be addressed and* ***designed-in from the start****, irrespective of the use case for the Blockchain …*
Nick*: We know that electronic voting systems are vulnerable to hacking. Can Blockchain-based voting systems also be hacked?*
Dr. Castell*: Anything can be hacked, and electronic voting systems are no different. …*
Nick*: Is it the Blockchain that could be compromised or is it more likely a voter's smartphone would be compromised by a hacker?*
Dr. Castell*: A well-engineered and implemented Blockchain distributed voting ledger should itself be as immune to compromise as its cryptography can provide. But the voter's smart phone security, and the overall voting application, are only as sound as whatever has been designed-in to the whole system … smartphones have … in the past been hacked. It is not clear that the proposed West Virginia smartphone application would be any more (or less) hackable than anything else hitherto.*
Nick*: What sort of checks and balances would you expect for a Blockchain-based voting system before implementation?*
Dr. Castell*: It would seem an obvious (constitutional?) requirement that* ***votes must always be manually-countable in any US election, in the event of suspected error or lack of trust in the reported result*** *... Lawyer Jonathan Bolls is a Magistrate, and Chief Election Officer, in Fairfax County, Virginia ...: "For Blockchain technology, where someone is voting on their phone from overseas, … they potentially waive their rights to have their vote counted should a re-count be necessary. We have actually … removed our high-tech touchscreen voting systems and returned to the paper ballot. If ever we need to check voting numbers we hand count". Aside from manual auditability, before implementation it is vital that 'Proof of Concept' projects be thoroughly executed, carefully trialing any proposed smartphone public voting system ... Such Pilot Trials or Proving Systems are essential …* ***monitored and carried out by independent experts.***
Nick*: In your expert opinion, would you trust a Blockchain-based voting system to accurately register votes?*
Dr. Castell*: Deliberate hacking or compromise apart, there is no reason why a well-engineered and implemented Blockchain-based voting system, with careful professional expert involvement in its design and trialing before go-live, should not accurately register votes. However, I do not consider that a so-called 'trustless' Blockchain-based voting system removes* ***the need for a Trusted Third Party*** *legally responsible for its operation and security.* ***'Who you gonna sue when it goes wrong?'*** *…*

Background:
https://arstechnica.com/tech-policy/2018/08/experts-criticize-west-virginias-plan-for-smartphone-voting/
HACK THE VOTE — Experts criticize West Virginia's plan for smartphone voting Startup claims it can use the blockchain to make Internet voting secure. TIMOTHY B. LEE - 8/7/2018
https://voatz.com https://venturebeat.com/2018/01/08/voatz-raises-2-2-million-to-make-elections-tamper-proof/
Voatz raises $2.2 million to make elections tamper-proof MO MARSHALL JANUARY 8, 2018
https://www.experts.com/Articles/Blockchain-vs-Trust-Cryptic-Expert-Issues-by-Stephen-Castell
http://jonathanbolls.blogspot.com/
https://authors.elsevier.com/a/1XSpq_654J6Hkp
Computer Law & Security Review, Volume 34, Issue 4, August 2018, Pages 739-753. *Landmark 200th issue of CLSR* under the Editorship of Emeritus Professor Steve Saxby.
'The future decisions of RoboJudge HHJ Arthur Ian Blockchain: Dread, delight or derision?' Stephen Castell. *As largely authored by his personal Castell GhostWriteBot.*
Can you tell if this paper has been authored by an AI robot? Would it matter, legally or otherwise, if you can't?
https://www.journals.elsevier.com/computer-law-and-security-review
https://www.southampton.ac.uk/law/about/staff/sjs.page

- Commission of the European Community. Green paper on the security of information systems, ver. 4.2.1, 1994.
- S. Castell, Code of practice and management guidelines for trusted third party services, INFOSEC Project Report S2101/02, 1993.

Please feel free to circulate, re-blog or retweet to your personal, business and professional contacts and communities, and by all means cite and reference.
Kind regards,
Stephen Castell.

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

http://www.national-experts.com/Members2/witness.asp?d_memnum=11599&d_lnum=1
CASTELL Consulting
IT CONSULTANT OF THE YEAR
Dr. Stephen Castell, CITP, CPhys, FIMA, MEWI
P.O. Box 270529, San Diego, CA 92198, Tel: (310) 890-9859
Expert Category: COMPUTERS/SOFTWARE - General
Specialties: IP, mobile technology patents, computer, software, telecommunications, broadcasting litigation/dispute resolution, Expert Witness, CEDR Mediator, ICC Arbitrator, Expert Determiner. …

Committee Member, Programme Development & IT Professionalism, British Computer Society Law Specialist Group
http://www.bcs.org/category/10868

Accredited Member, Forensic Expert Witness Association, *Los Angeles Chapter*

Dr Stephen Castell is an award-winning independent ICT expert witness, management consultant and project manager professional, with extensive experience in risk assessment, quality assurance, and dispute resolution. A pioneer of the Over The Counter Market in the UK, raising risk capital for new technology-based companies, he is a Panellist on CryptoBlockTV:
https://vimeo.com/user36208838/review/257927211/7ff86eed15

From: Dr Stephen P CASTELL [mailto:stephen@castellconsulting.com]
Sent: 13 August 2018 18:46
To: Friends and Colleagues (stephen@castellconsulting.com) <stephen@castellconsulting.com>
Subject: 'The future decisions of RoboJudge HHJ Arthur Ian Blockchain...'; CLSR, Vol 34, Issue 4, August 2018, Pp 739-753

CLSR celebrates its Landmark 200th Issue

Hello

I thought you would be interested in a softcopy of my paper contributed to the special 200th celebratory issue of *Computer Law and Security Review* (CLSR), at the invitation of its Founder and Editor-in-Chief, Emeritus Professor Steve Saxby (https://www.southampton.ac.uk/law/about/staff/sjs.page).

This special *CLSR* issue, in preparation for several months, has just been published by *Elsevier*, who have provided a personalized URL giving 50 days' free access to my article, titled "**The Future Decisions of RoboJudge HHJ Arthur Ian Blockchain: Dread, Delight or Derision?**". Anyone clicking on this link before September 16, 2018 will be taken directly to my article on *ScienceDirect* (no sign up, registration or fees are required – simply click and read):

https://authors.elsevier.com/a/1XSpq_654J6Hkp
Computer Law & Security Review, Volume 34, Issue 4, August 2018, Pages 739-753
'The future decisions of RoboJudge HHJ Arthur Ian Blockchain: Dread, delight or derision?'
Stephen Castell. ***As largely authored by his personal Castell GhostWriteBot. Can you tell if this paper has been authored by an AI robot? Would it matter, legally or otherwise, if you can't?***
A Contribution to the *Landmark 200th issue of CLSR* under the Editorship of Emeritus Professor Steve Saxby.

Abstract
Steve Saxby's prescient founding of *CLSR*, two hundred issues ago, encouraged and resonated with my own digital visionary thinking and professional activity in the evolving field of *ICT and the Law*. From *Infolex*, the UK's first commercially-available computer-assisted legal information retrieval service, and my *APPEAL Report* (on the admissibility of computer evidence in court and the legal reliability/security of IT systems), via my *Forensic Systems Analysis* expert methodology, to the nascent *CryptoBlockTV*, Steve's scholarly foresight in promoting adventurous exploration of 'digilaw' high-ground topics and issues has presented me with opportunities to generate a stream of prescient material, for which I am immensely grateful. And what is beyond prescient today is that the Coming of the Robots is unstoppable. The Artificial Intelligence (AI) Age is upon us; *RoboJudge* has all but already arrived. While many are concerned about defining and developing Machine Ethics, *Castell's Second Dictum: "You cannot construct an algorithm that will reliably decide whether or not any algorithm is ethical"* reveals that this is a futile exercise. Algorithms are also pivotal to the current mania for *Crypto-Algorithmic Blockchain Technology* Initial Coin Offerings (ICOs), with a 'Crypto Tribe' of Millennials relentlessly raising billions in real money thereby, to the extent that I have dubbed Crypto *the Millennials' Rock'n'Roll*. The seasoned ICT expert professional however bears in mind that there are as yet no ISO standards for blockchain, and there is far more to creating and delivering a complete quality-assured system than just the blockchain component. Furthermore, the legal status of cryptocurrency, smart contract and distributed ledger technology is not clear or uncontentious – and there is already ICO litigation on foot. Nevertheless, taking my limerick-writing *Castell GhostWriteBot*'s advice, it is perhaps time for my own asset-linked ICO, to launch my *CapChere.com* concept designed to reboot Capitalism and achieve *ubiquitous universal share and wealth ownership*. Look out for *Castell GhostWriteBot*'s account (with or without limericks) of how I fared, in the 400th issue of *CLSR*.

Contents

Keywords: Intelligence Blockchain Robot Ethic Algorithm Crypto
https://doi.org/10.1016/j.clsr.2018.05.011

Enjoy! And do please feel free to circulate to your colleagues and contacts.

Kind regards,
Stephen.

PS Cf. http://www.dailymail.co.uk/sciencetech/article-6000619/Can-spot-real-Shakespeare-sonnet-AI-learns-write-poetry.html
Can YOU spot the real Shakespearean sonnet? The AI learning how to write its own poetry 27 July 2018 By MARK PRIGG FOR DAILYMAIL.CO

- *Researchers at IBM used 2600 sonnets to train their AI*
- *Researchers asked workers from a crowdsourcing website to rate them*
- *Found they were unable to distinguish them from the real deal*

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
***Committee Member,** Programme Development & IT Professionalism, British Computer Society Law Specialist Group*
http://www.bcs.org/category/10868

https://www.journals.elsevier.com/computer-law-and-security-review
Computer Law & Security Review The International Journal of Technology Law and Practice Editor-in-Chief: Steve Saxby
The Computer Law and Security Review (CLSR) is an international journal of technology law and practice providing a major platform for publication of high quality research, policy and legal analysis within the field of IT law and computer security. It has been published six times a year since 1985 under its founding Editor, Professor Steve Saxby. It is the leading journal of its kind in Europe and provides a robust peer reviewed medium and policy forum for dissemination of knowledge and discussion, supported by powerful Editorial and Professional Boards and an Editor of more than 30 years specialist experience in the field. CLSR is accessible to a wide range of academics, researchers, research institutes, companies, libraries and governmental and non-governmental organisations in both the public and private sectors as well as professionals in the legal, IT and related business sectors in more than 100 countries. It is available on ScienceDirect, the world's foremost provider of electronic scientific information to more than 16 million subscribers. CLSR authors come from leading academics, international specialists, legal professionals and early career researchers from many of the most renowned research centres and universities in the world. Contributors are also located in the major international law firms, specializing in technology law, who provide essential comment and analysis built upon widespread experience of applying IT law in practice. … CLSR publishes refereed academic and practitioner papers on a wide range of legal topics such as Internet law, telecoms regulation, intellectual property, cyber-crime, surveillance and security, e-commerce, outsourcing, data protection, ePrivacy, EU and public sector ICT policy, and many others. In addition it provides a regular update on European Union developments, and national news from more than 20 jurisdictions in both Europe and the Pacific Rim. … All papers are … peer reviewed by relevant experts ... For further information please contact the Editor, Professor Stephen Saxby, Law School, Faculty of Business and Law, The University, Highfield, Southampton SO17 1BJ UK Tel/Ans: +44 (0) 23 8059 3404, s.j.saxby@soton.ac.uk