CASE NO.: D-16-NNNNNN-S

DISTRICT COURT
FAMILY DIVISION
CLARK COUNTY, NEVADA

BETWEEN

CAROLINE LA PLACE (NKA CAROLINE SHEAKELL)
("CLP")

<u>**Plaintiff**</u>

-and-

RODERICK LA PLACE
("RLP")

<u>**Defendant**</u>

_____

Expert's Report
19 October 2020

_____

Prepared for:-	Amanda M. Roberts, Esq. *Roberts Stoffel Family Law Group* 4411 S. Pecos Road, Las Vegas Nevada 89121, United States of America www.lvfamilylaw.com Phone No.: +1 (702) 474-7007 Fax No.: +1 (702) 474-7477 E: amanda@lvfamilylaw.com
Prepared by:-	*CASTELL Consulting* (Castell Computer and Systems Telecommunications Ltd) PO Box 334, Witham Essex CM8 3LP, United Kingdom Tel: +44 1621 891 776 Mobile: +44 7831 349 162 Email: stephen@castellconsulting.com *www.CASTELLConsulting.com*
Author:-	Dr Stephen Castell

Notice

This **Expert's Report** has been prepared in connection with the matter of *La Place -v- La Place*. It is not intended, and should not be used, for any other purpose. Any opinions expressed by the author herein are presented for this purpose alone, and may be subject to modification or deletion in the light of further information and investigation. These opinions are based solely on reviews of people, documentation, systems and other information as supplied or made available to *CASTELL Consulting*.

CASE NO.: D-16-NNNNNN-S

<div align="center">

DISTRICT COURT
FAMILY DIVISION
CLARK COUNTY, NEVADA

</div>

BETWEEN

<div align="center">

CAROLINE LA PLACE (NKA CAROLINE SHEAKELL)
("CLP")

</div>

Plaintiff

<div align="center">

-and-

RODERICK LA PLACE
("RLP")

</div>

Defendant

_____

<div align="center">

Expert's Report
19 October 2020

</div>

_____

CONTENTS   **PAGE**

1.   Introduction and Background

- **I, Stephen Peter Castell, submit the following report declaring my opinions related to those technical issues and case documentation which I have been instructed to examine, as arising from the pleaded cases of the parties in this *La Place v La Place* matter.**
- **This report provides the opinions, about which I may testify at the Trial on behalf of RLP, in regard to these issues, as well as the bases of those opinions. This report is based on my study, examinations, investigations, expertise and experience to date, and sets forth the testimony that I am likely to present regarding my opinions.**
- **I may also present testimony in further rebuttal to the testimony and evidence that CLP presents.**

1.1   Personal Information

Personal Details

1. I, Stephen Peter Castell, am a Chartered IT Professional and an independent consultant in computer and telecommunications systems and software development. I am Chairman of the United Kingdom company CASTELL Computer and Systems Telecommunications Limited ('*CASTELL*' or '*CASTELL Consulting*'), a professional firm of Management and Financial Consultants in Information Technology of over 40 years' standing. I am an expert in the specification, design, development, project direction and contract management of computer applications software; in areas of Information & Communications Technology ('ICT') and software applications industry custom and practice; in analysis of value and other assessments of software, systems and ICT outsourcing and other supply agreements; and in forensic examination of data and other records in respect of the validity, development and use of computer and telecommunications systems, of the consequences of such use, and the inferences and conclusions to be drawn from them. I have been instructed as an expert witness on a wide range of ICT and ICT services assignments, and related litigious and non-litigious disputes, and in particular, for example, in software copyright, and ICT technology patent, disputes, and in computer software and systems litigation; for both Plaintiffs, Claimants or Pursuers, and Defendants, Respondents or Defenders, and for both purchasers/users and providers/suppliers of ICT software, systems and services, and on behalf of insurers, in the UK and internationally.

2. My qualifications, experience and a note of some of the cases on which I have been instructed as expert are given at *Appendix ONE*: **Dr Stephen Castell – qualifications and experience** of this **Expert's Report**.

Authorship of this Expert's Report

3. I have personally carried out or directed all work undertaken in regard to my investigations, analyses and findings. I confirm that the conclusions and opinions expressed herein are entirely my own.

1.2   Background to the Dispute and my Appointment

4. I was on October 09th, 2020, appointed and instructed by Attorney Amanda Roberts of *Roberts Stoffel Family Law Group*, to produce an independent expert's report on behalf of her client, the Defendant, RLP, to be delivered by Monday October 19th, 2020. I understand from Attorney Roberts that the background to this case is that RLP was divorced from the Plaintiff, CLP, by Decree Absolute, in connection with which a dispute has arisen between them over potential digital assets of RLP said to be holdings of, and transactions in, cryptocurrencies, in particular Bitcoin.

5. I further understand that a Second Supplemental Post Decree Disclosure of Witnesses and Documents, pursuant to NRCP 16.2, was submitted to the DISTRICT COURT, FAMILY DIVISION, CLARK COUNTY, NEVADA, consisting substantively of the ***Expert Report dated 5/28/2020 by Robin A. Shilson*** ('the Shilson Report').

6. I am asked to
  - Review the Shilson Report together with consideration of case documentation provided to me by Attorney Amanda Roberts.
  - Produce a high-level critique of the Shilson Report, giving such insights, analyses, findings, conclusions and opinions as may be sensibly achievable in the relatively limited timescale and associated effort and budget available for my work. It is agreed that these examinations will not include carrying out my own technical investigation or research on or into the specific or detailed software forensics, cryptocurrency trading, wallet etc instances referred to within the Shilson Report.
  - Provide an overview and explanation of the blockchain and cryptocurrency, crypto assets etc field to assist the understanding of the Court, in respect of principally a general introduction, plus as regards technical issues relevant in the case.

7. This **Expert's Report** is my account of the review that I have carried out, giving, as instructed, my explanations, findings, conclusions and opinions.

1.3   Statement of Impartiality

8. Prior to being appointed in this case, I have not worked or acted in any capacity for or on behalf of RLP, or CLP, or with regard to any matter in which they were or are involved. I believe that in this report the facts I have stated are true and the opinions I have expressed are correct.

9. I understand that my overriding duty is to assist the Court on matters that are within my expertise. I also understand that this duty overrides any obligation to *Roberts Stoffel Family Law Group*, who act for RLP in this matter, or their clients.

10. I further confirm that I have at all times conducted, and will at all times conduct, my expert inspections and examinations pursuant to the expected standards of impartiality and independence.

2.   Research Methodology

2.1   Documents Reviewed

11. On October 09th, 2020, I was provided with the documents given at *Appendix TWO*: **Documents Provided and Reviewed in this Report** of this **Expert's Report**.

12. Where I make reference herein to a page or pages of any one of these documents, this is in one of the formats:
> 'n/N; <Pdf ID>': where n is the pdf page number in question located within the total of N pages in the document with 'Pdf ID'; or
> 'P <page number(s) within document> <Document ID>', where 'Document ID' is as given in the following table:

Document ID	Total Pages
Shilson Report	23
ORDER FREEZING ASSETS	2
SUBPOENA DUCES TECUM TO COINBASE	12
CLP'S SUPPLEMENTAL PRODUCTION	3
Letter from Coinbase June 18-2018	3
Coinbase Account Statement 1: 01/23/2015-03/23/2018	8
Coinbase Account Statement 2: 02/16/2015-07/25/2018	2
Coinbase Account Statement 3: 06/01/2016-07/25/2018	1
Letter from Carter [Poloniex] January 12-2018	1
Poloniex Statement - 'Entity 99NNN Account #100NNNNN'	53
Poloniex KYC ID for RLP	2
Poloniex DECLARATION OF CUSTODIAN OF RECORDS	1
CLP'S PRODUCTION OF DOCUMENTS	79
DEPOSITION OF RLP	37
CLP'S FIRST INTERROGATORIES TO RLP	5
CLP'S REQUESTS FOR ADMISSIONS TO RLP	3
CLP'S FIRST REQUEST FOR PRODUCTION OF DOCUMENTS TO RLP	2
SUBPOENA TO COINBASE	5
SUBPOENA TO POLONIEX	5

2.2   Investigations Carried Out

13. The investigations that I have carried out have consisted of
- Reading and considering the documentation supplied to me, as given at *Appendix TWO*: **Documents Provided and Reviewed in this Report** of this **Expert's Report**.
- Some limited literature, web etc research.

3.   Issues addressed in this Expert's Report

14. This **Expert's Report** provides an account of my investigations, analyses, and findings in regard to my instructions to
- Review the Shilson Report together with consideration of the case documentation provided.
- Produce a high-level critique of the Shilson Report.
- Provide an introduction to the blockchain and cryptocurrency, crypto assets etc field to assist the understanding of the Court.

15. The relevant technical requirements that fall within my field of expertise are the computer software and systems aspects of the Shilson Report and in particular of the blockchain and cryptocurrency, crypto assets etc field.

16. I make it clear that I am not a capital or currency market trading professional or financial advisor, and neither offer nor provide investment advice. Neither do I have any commercial interest in or management connections with any cryptocurrency, cryptocurrency trading exchange or any operators of such entities or promotors of associated businesses.

4.   Analysis and Findings

4.1 The Instructions to Mr Shilson and the Scope of the Shilson Report

4.1.1 Introduction to Blockchain and Cryptocurrency

17.   In simple terms, blockchain is the computer software and systems technology that (among other things) enables the existence of cryptocurrency. Bitcoin is the name of the best-known cryptocurrency, being the cryptocurrency for which blockchain technology was originally developed.   Like the USD, a cryptocurrency is a medium of financial value exchange, but it is digital and uses encryption techniques to control the creation of monetary units and to verify the transfer of funds.

18.   A blockchain is a software and systems application that provides a decentralized ledger of all transactions across a peer-to-peer network. The key principle of using blockchain is that participants can confirm transactions without a need for a central clearing authority. Potential applications in the financial and investment sector can include fund transfers, and settling trades.   Other application areas, or 'use cases', for blockchain are myriad, and include voting, supply chain logistics management and health informatics.

19.   Blockchain thus has potential applications far beyond Bitcoin and cryptocurrency. From a general business perspective, blockchain technology may be thought of as a type of next-generation business process improvement software.   'Collaborative technology' such as blockchain can offer the ability to improve the business processes that occur between companies, significantly lowering the 'cost of trust'.   For this reason, there is a growing management and investor realization that, in the right use cases, blockchain may offer substantially higher returns 'for each investment dollar spent' than many traditional corporate internal technology investments.

20.   I set out further basic introduction to and explanation of blockchain and cryptocurrency in general, and Bitcoin in particular, in ***Addendum A*: Introduction to Blockchain and Cryptocurrency** of this **Expert's Report**.

4.1.2 Valuation of Crypto Assets

21.   Mr Robin A Shilson ('RAS') does not provide a CV in his report, the Shilson Report. From simply some brief online research, I have achieved an understanding of his qualifications and experience which I set out in ***Appendix THREE*: Qualifications and experience of Mr Robin A Shilson** hereof. This understanding may of course, to some extent or other, be inaccurate and/or incomplete, but, absent any details provided by RAS himself in the Shilson Report, I here rely on it.

22.   From this material I take that the career background and core competence of RAS as an expert witness retained on behalf of the Plaintiff in this *La Place v La Place* case is in brief "*a blockchain forensics expert and cryptocurrency cybercrime investigator with experience in dozens of cases*".

23.   RAS states on P 1 Shilson Report "I have been asked by Richard K. South, Counsel for Caroline Sheakell, to perform an analysis of cryptocurrency holdings of Roderick J. La Place". RAS does not give any further details of the nature, scope or purpose of his instructing attorney's request "to perform an analysis of cryptocurrency holdings".

24.   Given that the analysis of cryptocurrency holdings of RLP is intended to be relevant, as I understand it, in the context and for the purpose of identification, understanding, confirmation, and valuation of, in particular, such crypto assets of RLP as may be decided by the Court are assessable in regard to the settlement of disputes arising between the parties pursuant to their Divorce Decree, I venture to surmise that the principal technical issue that RAS may have implicitly been instructed to address might reasonably have been expressed along the lines of:

<u>The Issue for Experts</u>

"Based on the documents provided and evidence disclosed in the case:

(i)   What were, at a defined date, or dates, the cryptocurrency holdings of Roderick J. La Place.

(ii)   Where are these crypto assets held today.

(iii)   What are the technical processes or protocols through and by which such crypto assets would be accessible and potentially realizable in US Dollars or other fiat currency."

25.   I can envisage that a Second Issue could be of importance in the context of settlement of disputes arising between the parties pursuant to their Divorce Decree, namely, something along the lines of "What was, at a defined date, or dates, a relevant reasonable valuation in US Dollars or other fiat currency of the cryptocurrency holdings of Roderick J. La Place?". However, in my experience, the matter of valuation of digital assets (whether data, software, or some combination thereof) is a complex field, with many legitimate financial assessment and accounting models and methodologies available to and employed by suitably skilled experts, which, dependent on all the facts and circumstances, can be both competing and complementary in pursuit of arriving at an objectively justifiable value.

26.   For example, for a recent software investment scheme dispute, heard in the First Tier Tax Tribunal in the UK (and currently proceeding to Appeal), I was retained as a digital asset valuation expert to provide an opinion on the value of certain software assets, the subject of Exchequer investment tax advantage schemes with reliefs claimed in hundreds of millions of GBP. I there identified, from my own relevant active client experience, and from knowledge of the literature and scholarly research on the subject, together with applicable industry custom and practice, at least <u>six different distinct valuation methodologies</u>.

27.   Each of these methods are equally potentially legitimate and applicable. They are, and have over the past forty years of the digital industries and commerce been, variously and routinely used by financial accountants, auditors, investment analyst professionals, digital technology company management, deal negotiators and software cost modeling specialists, singly or in combination and cross-check, to arrive at valuations of software digital assets for a variety of trading, business, resourcing, forensic, tax and regulatory purposes.

28.   However, whatever the methodology or methodologies to be used by an expert to arrive at a valuation of digital assets (or, more usually, and properly, a range of valuations; and always fully disclosing and explaining clearly the methodologies used, and their justification in the particular circumstances of the case), in my experience it would be for the Court to decide first, having heard and taken into account such available expert and other testimony as the Court wished, what exactly are, or were the subject assets (here, cryptocurrency holdings), i.e. what precisely *is* the schedule of the assets that is to be held to be assessable in the case, usually before any expert valuation of them is carried out.

29.   Therefore, since it is not clear that the opening statement by RAS that "I have been asked by Richard K. South, Counsel for Caroline Sheakell, to perform an analysis of cryptocurrency holdings of Roderick J. La Place" specifies that RAS was instructed to address this hypothetical Second Issue, and since I see nothing in what I have (perhaps incompletely) discovered about the qualifications and experience of RAS which speaks particularly to skills and competence as an expert in carrying out and giving opinion on digital (data, and/or software), assets valuation, including therefore crypto assets, I assume for the purposes of this my **Expert's Report** that any analyses, findings, conclusions or opinions explored or provided by RAS in the Shilson Report concerning the *values*, or *valuations*, of "cryptocurrency holdings of Roderick J. La Place" were and are outside the scope of his instructions, and they should be ignored and properly not be within the compass of my work for this **Expert's Report**.

4.1.3 Suggestions of potential criminal activity

30.   To re-iterate, on P 1 Shilson Report the opening statement describing the instructions given to RAS by his instructing attorney is "I have been asked by Richard K. South, Counsel for Caroline Sheakell, to perform an analysis of cryptocurrency holdings of Roderick J. La Place".

31.   This makes no mention of RAS being asked to consider or analyze either the possible motivation of RLP, and/or the honesty (or otherwise), and/or the potential criminality of RLP's activities in regard to his cryptocurrency holdings, their disclosure, trading and/or associated transactions. Nor does it request RAS to make any analysis, finding, comment or opinion as to whether or not RLP personally has been 'forthright', 'honest', making 'attempts of concealment' or 'clear attempts to conceal his cryptocurrency', exhibiting conduct that 'may have implications of law enforcement interest', and/or 'has not provided truthful nor complete answers regarding his cryptocurrency holdings'.

32.   Furthermore, I have seen no qualifications stated of RAS as an expert in, say, Motivational Psychology, nor as an Honesty or Integrity Assessment Professional, nor as an Investigator in Fraudulent Intent Discernment, nor as a Criminality Analyzer, nor as a Behavioral Scientist or Practitioner. In short, I am not aware that RAS has, or professes, any skills, training, qualifications or experience as a Forensic Psychologist (for example, the type of professional who may be a member of https://www.myiacfp.org/). His skillset and experience appears to be centered on, as he himself puts it on his own website: "*mapping blockchain transactions and explaining the movement of assets to laymen with little or no blockchain experience in a way that simply makes sense, with meticulously constructed graphics to illustrate typically hard-to-understand flows in an easily interpreted way*".

33.   I may have misunderstood, but it also does not seem to me to be the case that RAS is skilled, trained or has any official standing as a Law Enforcement Officer or Agent and, even if perhaps he is some sort of secret officially-appointed Crime Investigator, or possibly an associate, or even 'undercover', operative on behalf of, say, the Police or another Law Enforcement Organization, as far as I can discern he has not declared, disclosed or represented himself as such within his published CV material – let alone within the Shilson Report, his expert testimony for this *La Place v La Place* case.

34.   Finally, I understand that this *La Place v La Place* case is a Civil Law matter, being heard in a District Court, Family Division; it is not a Criminal Law action being brought by Prosecutors in a Criminal Court. In my experience, in an Expert's Report for a Civil Law matter there is no place or justification for a technical expert, requested and instructed, and with overriding duty, to assist the Court on matters that are within his expertise, to go beyond this.

35.   Such a technical expert should therefore not in my view and experience venture suggestions of potential criminal activity, or intent, on the part of any party in the subject Civil Law dispute. Such suggestions could include alleging lack of being honest or forthright, or hinting at negligent or fraudulent misrepresentation, or propounding that a party has been tampering with or hiding evidence: all such, and similar, statements or innuendos are, in my experience, inappropriate, unwanted and unwarranted in an expert report of which, as I understand it, the Shilson Report is intended to be an example.

36.   I have personally been professionally involved with an English High Court case (claiming large damages and other compensation for alleged failure of a major software development) where a much respected and seasoned ICT professional acted as expert witness for Party A, opposing Party B on whose behalf I was engaged, in which, in his Expert's Report, he, unusually and alarmingly, opined that Party B's programmers had with deliberate dishonest intent incorrectly programmed the system such that it would not pass User Acceptance Testing, to create 'false faults' in the system in order that the development contract would be extended and more money spent with Party B to fix the faults. Such was the seriousness of these allegations by a leading technical expert that the Main Board of Directors of Party B (one of the largest publicly-listed UK corporations) became involved, and, had the expert for Party A not reconsidered, and (after I met with him, without prejudice, and explained clearly to him that he was simply misinterpreting certain technical evidence) withdrawn his allegations, the Main Board would have sought formal sanction of that respected expert by the Court for giving unwarranted, unfounded and arguably defamatory opinion which was also outside the ambit of his instructions. (As a sad footnote, that expert, a long-time ICT consultant and expert professional colleague of mine, died from cancer, less than a year after that case was settled, in favor of my client, Party B).

37.   Therefore, I further assume for the purposes of this my **Expert's Report** that any suggestions of potential criminal intent or activity, as explored, made or hinted at by RAS in the Shilson Report, were and are outside the scope of his instructions, and they should be ignored and properly not be within the compass of my work for this **Expert's Report**.

4.2 Review of the Shilson Report

4.2.1 Evidence upon which the Shilson Report is based

38. Having commenced his report by stating his instructions, on P 1 Shilson Report, as "I have been asked by Richard K. South, Counsel for Caroline Sheakell, to perform an analysis of cryptocurrency holdings of Roderick J. La Place", and having confirmed on the title page that it gives an account of an "Analysis of Cryptocurrency Transacted and/or Owned by Mr. La Place", RAS continues "To assist in the accomplishment of this task, I was provided with a variety of documents, some of which were obtained via subpoena from Coinbase and Poloniex. These documents include information regarding Mr. La Place's accounts on the aforementioned platforms; namely, cryptocurrency deposits and withdrawals".

39. RAS goes on to explain "The documents reviewed were as follows:", and then gives a table listing details of eleven documents under column headings:

Type or Source	Title or Description	Page Count	Date

I can see that these documents appear by title, page count and date to be substantively if not exactly the same as those provided to me by my instructing attorney, as listed within the table I have given at ***Appendix TWO*: Documents Provided and Reviewed in this Report** of this **Expert's Report**.

40. It does seem therefore that RAS has been asked to "to perform an analysis of cryptocurrency holdings of Roderick J. La Place", and thereby arrive at conclusions and opinions of relevance and assistance to the Court in settlement of the Civil Law dispute arising between the parties pursuant to their Divorce Decree, based on essentially, and only, the same documents as I have been asked to consider.

41. However, having read through the whole of the text of the Shilson Report, in which RAS sets out many examples of individual cryptocurrency holdings and transactions, with some kind of analyses carried out on them, and inferences drawn from them, I can find only the following two places where, in presenting the specific data and assertions on which his workings are then developed, there is any actual, or navigable, reference given by RAS into the documents on which he was instructed to rely:

P 13 Shilson Report: "The Poloniex withdrawal history".

P 13 Shilson Report: "demonstrates a level of frequent day-trading and chatter … [in] the multiple pages of transcripts in the documents Poloniex provided"

If I understand correctly, these two references are intended to be to the <u>whole</u> of the 53 pages of the Poloniex Statement - 'Entity 99NNN Account #100NNNNN' document.

42. As far as I can discern, apart from these two instances of reference, and to that whole document, not one of the 31 other uses of the word 'Poloniex' in the Shilson Report provides a precise reference into the specific page, and/or element on that page, on which RAS relies when citing 'Poloniex'. It is impossible therefore to go direct to a specific element of Poloniex-supplied evidence and check whether what RAS asserts, purporting to rely in the Shilson Report on that element, is, or is not, accurately quoted, or whatever else.

43. Just a couple of examples of this lack of precision, and thus of the impossibility of directly checking the evidence upon which RAS is relying, and thereby beginning to understand the point he then goes on to develop, are:

P 8 Shilson Report: "This was identified via following a blockchain trail from a Poloniex withdrawal" – this is vague: which 'trail', and which 'withdrawal'? No reference is given to a page within the 53 pages of the Poloniex Statement - 'Entity 99NNN Account #100NNNNN'.

P 12 Shilson Report: "Mr. La Place withdrew approximately 290 XMR16 from his Poloniex account between October 30th, 2017 and November 8th, 2017" – this also is vague: 'withdrew' when exactly? No reference to a page number within the 53 pages of the Poloniex Statement - 'Entity 99NNN Account #100NNNNN' document is given.

4.2.2 Review of online chat messages within the Shilson Report

44. At P 14 Shilson Report RAS begins a section headed 'Ill. OFF-CHAIN OBSERVATIONS', which commences with the comment that "Mr. La Place demonstrates a level of …. chatter".

45. For the next two pages, P14-16, i.e. around 10% of the content of the whole Shilson Report, RAS simply reviews free-form 'chat message' items apparently drawn from entries in the 'Chat Log' section, P 36-52 Poloniex Statement - 'Entity 99NNN Account #100NNNNN' document – although, once again, there is not a single page number or other specific reference, e.g. table entry, given by RAS enabling the existence or accuracy of the elements of 'chat' evidence quoted by him and on which he relies to be checked.

46. A read through the whole of this 'Chat Log' confirms that it is exactly that – a record of chatter and messages of a largely informal character. In my understanding and to the best of my knowledge such conversational chat content is rarely of any contractual or technical significance, and in my view and experience it should thus be given little weight in regard to an expert 'analysis of cryptocurrency holdings'. Furthermore, it is common experience and knowledge that 'chat messages', when exchanged in private, as here between RLP and Poloniex, are often expressed without much care or thought, possibly in a hurry, and should sensibly not be regarded as anything other than essentially of a 'casual' nature.

47. In my view and experience such content cannot be taken as technically reliable, and the 10% of the Shilson Report which dwells on it should, I respectfully suggest, be considered to be discounted by the Court in terms of its relevance to or providing expert testimony of assistance with deciding the issues to be tried in this *La Place v La Place* case.

4.2.3 Reliance on undisclosed documents, evidence or sources in the Shilson Report

48. Furthermore, RAS seems to have relied on other documents, evidence or sources which he has not disclosed in the Shilson Report, examples being:

P 16 Shilson Report: "There are a number of important observations not inherently associated with the Poloniex documents:" – it is not disclosed from which documents these 'important observations' are derived, or upon which they rely, given it is asserted that they are not 'inherently' within the 53 pages of the Poloniex Statement - 'Entity 99NNN Account #100NNNNN' document.

P 16 Shilson Report: "I am informed that no ICO early investment was discussed nor mutually agreed upon" – by whom, and how, was RAS so 'informed'?

49. There is what amounts to a whole page of such content, i.e. around 5% of the content of the whole Shilson Report, beginning at P 16 Shilson Report: "There are a number of important observations not inherently associated with the Poloniex documents:", and ending at P 17 Shilson Report: "5. It appears possible that Mr. La Place sold property approximately July of 2019 …".

50. In my view and experience such content, based on undisclosed, unexplained and unreferenced documents, evidence or sources cannot and should not be relied upon, and the 5% of the Shilson Report which dwells on it ought, I respectfully suggest, to be considered to be discounted by the Court in terms of its relevance to or providing expert testimony of assistance with deciding the issues to be tried in this *La Place v La Place* case.

4.2.4 Shilson Report content going outside the scope of expert instructions

51. At P 17-21 Shilson Report, some three pages, around 14% of the content of the whole Shilson Report, there is a section headed '**IV. RECOMMENDED COURSES OF ACTION**' which opens with the assertion by RAS that "It is my assessment the following actions would **push this case forward**:". **[My added emphasis]**

52. This whole section in my view presents uncomfortable difficulties in terms of the credibility of RAS as an independent expert witness. It contains what appears to me to be subjective, speculative, unfounded, prejudiced and/or pejorative material that I consider has no place in a report from an independent technical expert witness asked simply to "to perform an analysis of cryptocurrency holdings of Roderick J. La Place" based on the documents provided to him.

53. Furthermore, even leaving aside the subjective, speculative, prejudiced and/or pejorative nature of these assertions and comments, in my view RAS may here be in danger of being perceived as having gone outside the scope of his expert instructions "to perform an analysis of cryptocurrency holdings of Roderick J. La Place".

54. These assertions and comments include, by way of illustration (all falling within P 17-21 Shilson Report):
"This would most likely be either another cryptocurrency exchange…";
"If Mr. La Place is unable or unwilling to perform the above steps, it is likely that he is unwilling to do so for a concerning reason. This may include account ownership on a yet-unidentified cryptocurrency exchange.";
"If Mr. La Place is not willing to provide *complete* logs for whichever wallets, exchanges, and/or services utilized for procurement and/or storage of XMR, I would find this particularly concerning. ";
"It is possible that Mr. La Place took to selling cryptocurrency P2P or OTC for cash";
"Mr. La Place demonstrates a propensity to intermingle funds.";
"It is believed that Mr. La Place held varied corporations based out of Nevada";
"it is possible this account was used to conceal activity of interest to this matter";
"it is likely that Mr. La Place deposited Bitcoin to a GDAX address";
"This means it is likely that Mr. La Place has wallets for these cryptocurrencies";

"A day trader at Mr. La Place's level most likely invested in ICOs";

"it's incredibly unlikely Mr. La Place didn't own some level of Ethereum";

"Upon review of Mr. La Place's Telegram handle, it was discovered he is in the Celsius29 project's unofficial Telegram channel. … it is assessed as possible that Mr. La Place, at a minimum, registered with Celsius, and quite possibly has cryptocurrency holdings on the same.";

"This almost certainly is deliberate laundering attempt, as Mr. La Place likely believed he could hide this Bitcoin but naively withdrew to another wallet"; and

"It is possible Mr. La Place utilized numerous accounts with KuCoin (as well as other exchanges) to avoid KYC requirements".

55. In my view RAS may also here be in danger of being regarded as abrogating his objectivity and independence as an expert witness. He appears to me possibly to be purporting to act as an advocate, and/or also some kind of strategic advisor to an 'open investigation' of RLP unrelated to the issues in this *La Place v La Place* case. He begins by averring that his "recommended courses of action" are intended to "push this case forward". In 30+ years of acting as an expert witness I have never seen such phraseology used before in an expert report. In my view and experience it is not for an expert witness, who has to be (seen to be) independent and to honor his or her overriding duty to the Court, to be enthusing or advocating for a case to be 'pushed forward'. My understanding has always been that an expert witness must be disinterested (financially, and in all other ways) in the outcome of the case, and in how the case is decided to be progressed or 'pushed forward', and, indeed, in whether or not it is pursued further at all. Those are matters for the attorneys, the advocates, involved in the case, and I am clear that an expert witness must not be, or become, an advocate.

56. 'Push Forward' advocacy recommendations, assertions and comments made by RAS include, by way of illustration (all falling within P 17-21 Shilson Report):

"Subpoena Factom for any and all records associated with Mr. La Place's claimed participation";

"Subpoena any and all bank accounts owned and operated by Mr. La Place";

"Subpoena Coinbase for the following additional data";

"It would be imperative to perform analysis on any wallet addresses generated within GDAX by Mr. La Place.";

"Subpoena Poloniex for the following additional data:";

"it is advised that Mr. La Place be asked to provide information about where these loans were initiated and all pertinent details regarding said loans";

"Demand that Mr. La Place provide wallet addresses for cryptocurrencies not identified in the provided documents";

"Subpoena any and all brokerage accounts owned by Mr. La Place"; and

"Subpoena any and all company records for Sunshine Windows".

57. I consider that, RAS, advocating for further investigation and legal process by way of making these assertions, comments and recommendations, is at risk of being seen to demonstrate bias – unacceptable for a technical expert witness engaged with an overriding duty objectively, and with no personal agenda, to assist the Court. In my view and experience a perceived apparently biased position on the part of RAS as expressed here demands that the 14% of the Shilson Report in which RAS sets out his "recommended courses of action" should be discounted in terms of its relevance to or providing expert testimony of assistance with deciding the issues in this *La Place v La Place* case.

4.2.4 Insinuations in the Shilson Report of Criminality on the part of RLP

58.   Beginning at P 21 Shilson Report, and stretching over its concluding two pages, i.e. around 10% of the content of the whole Shilson Report, there is a final section headed 'V. SUMMARY STATEMENT' which opens, and closes, by stating what I take to be among the principal conclusions and opinions of RAS resulting from his analytical investigations:

P 21 Shilson Report: "Mr. La Place's actions demonstrate dishonesty regarding his cryptocurrency dealings."; and
P 22 Shilson Report: "Mr. La Place has not provided truthful nor complete answers regarding his cryptocurrency holdings".

59.   Given that the analysis of cryptocurrency holdings that RAS was requested to undertake was intended to be performed, as I understand it, in the context and for the purpose of identification, understanding, confirmation, and valuation of, in particular, such crypto assets of RLP as may be decided by the Court are assessable in regard to the settlement of disputes arising between the parties pursuant to their Divorce Decree, in my view these principal conclusions and opinions, as presented in the Shilson Report, focused as they are on issues of 'dishonesty', and 'truth', fail to provide any relevant assistive insights.

60.   Furthermore, within P 21-22 Shilson Report RAS makes comments that in my view and experience amount to insinuations that go beyond not merely of 'dishonesty', but of criminality, including as to whether or not RLP personally has been 'forthright', 'honest', making 'attempts of concealment' or 'clear attempts to conceal his cryptocurrency', exhibiting conduct that 'may have implications of law enforcement interest', and/or 'has not provided truthful nor complete answers regarding his cryptocurrency holdings'.

61. Earlier, at P 6 Shilson Report, RAS makes an even more serious suggestion:
"Mr. La Place may have been purchasing some type of illegal good on the dark web, which could be a range of possibilities from drugs to false identity documents".

62. And at P 17 Shilson Report RAS repeats and emphasizes hints of illegalities:
"c. This is common practice for those involved in suspect or illicit activity, and has been observed in *every* investigation of the same. In essence, these actions resemble what people do when they're doing the wrong thing via decreasing their footprint, potentially including destruction of evidence".

63.   A further, and extreme, example of such insinuations, actually amounting in my view to a pejorative inferential allegation of systemic illegality, criminality, and behavioural defects on the part of RLP, is at P 16 Shilson Report where RAS states:
"A review of public records for Mr. La Place presented the following:
a. Case number 99NNNNN in the California Los Angeles Superior Court for exceeding maximum speed of 65 MPH. … It is worth noting that there is a strong presence of speeding or other traffic violations in *nearly all* individuals I have investigated for white collar crime. The callous disregard for the safety of others, as well as impulsive decision making, are shared psychological attributes of a compulsive gambler".

64.   The insinuation that this passage appears to promote to the reader is that RLP is, or has been, involved in 'white collar crime', on presumably the premise that RAS has been instructed to 'investigate' RLP as an individual potentially involved in such white collar crime – which, however, as far as I understand the instructions to RAS, is simply not the case.

65.   That aside, I note once again that, as far as I am aware, RAS has no professional standing as a Forensic Psychologist, nor experience as a Behavioural Scientist, and I cannot see that he is qualified to opine as to whether or not any 'psychological attribute' of RLP is that of a 'compulsive gambler', nor in any event what this personally disparaging point has to do with fulfilling instructions "to perform an analysis of cryptocurrency holdings".

66.   In my view and experience such statements all appear to go outside what I understand are the instructions to RAS as a technical expert witness in this case, and I consider that they are unjustified and out of place. They cannot and should not be relied upon, and the 10% of the Shilson Report which this content represents ought in my view to be discounted in terms of its relevance to providing assistance with deciding the issues in this *La Place v La Place* case.

4.2.5 The 'blockchain forensics' and other software and analytical tools used in the Shilson Report

'analysis'

67.   RAS was asked "to perform an analysis of cryptocurrency holdings", and, as far as I can discern, in addition to appearances in the title page and in the declaration of instructions on P 1 Shilson Report, 'analysis' is mentioned seven times within its twenty-two pages:

(1)   P 2 Shilson Report: "this report will *not* conduct an **analysis** of the trading activity or other profit-taking initiatives of Mr. La Place".

(2)   P 2 Shilson Report: "2. Bearing in mind the objective of a finite report length, the inefficiency of doing by-trade **analysis** would not be judicious use of **our** expertise". This suggests, by use of the possessive pronoun "our" that RAS may have been assisted by others, with, presumably, relevant expertise, in the work of analysis for and production of the Shilson Report ('we' is also used seven times in the Shilson Report: 2 x P 5, P 6, 3 x P 11, and P 18; for example P 2: "the implications of what **we** are about to report"). If so, I would expect the identity, scope and nature of that assistance to have been disclosed. In any event this expression to my mind raises a doubt as to whether or not RAS has personally, and alone, carried out or directed all work undertaken in regard to his investigations, analyses and findings, and as to if the conclusions and opinions expressed in the Shilson Report are entirely his own.

(3)   P 2 Shilson Report: "This **analysis** is of cryptocurrencies of which Mr. La Place deposited or withdrew from these exchanges".

(4)   P 7 Shilson Report: "upon performing **analysis** of all of these wallets, it seems to be the case that Mr. La Place was utilizing a Bitcoin mixer".

(5)   P 7 Shilson Report: "… it would be possible to expand this section as much as double in length with even further **analysis** …".

(6) P 18 Shilson Report: "ii. … It would be imperative to perform **analysis** on any wallet addresses generated within GDAX by Mr. La Place".

(7) P 21 Shilson Report: "In the course of this form of **analysis**, indicators are silver, but data is gold".

(There are no variants of 'analysis', such as 'analyses', 'analyse', 'analyze', or 'analytical').

68. Numbers (1), (2), (5) and (6) above seem to refer to analyses which RAS has *not* done (or at least, not yet). It is only in three instances, numbers (3), (4) and (7) above, that RAS refers in the Shilson Report to actually having carried out an 'analysis'. As far as I can discover, at none of these places of use of the word 'analysis', or indeed elsewhere in the Shilson Report, is there given any of the usually-expected details as to exactly what analysis *was* actually carried out. By 'usually-expected details' I mean, for example: upon what science-based or other methodology was the analysis founded, what were the steps and processes in the analysis, what techniques or tools were employed, what software, if any, was used (the identification thereof, whose software, what version, parameters, set-up, operational environment), what results were obtained, what rationale, tools and techniques were used in interpretation of and conclusions drawn from the results, and so on.

69. At many places throughout the Shilson Report there are introduced and declared items or features of cryptocurrency data, using terminology such as wallets, addresses, amounts of Bitcoin, withdrawals, clusters, accounts, exchanges, services, funds, transactions, holdings, and worth, with inferences drawn by RAS from them, comments made about them and conclusions posited. However I have been unable to discover a single instance of the many assertions by RAS of such items where RAS materially gives or meaningfully explains the 'analysis' that he carried out thereon and upon which he bases his comments and arrives at his conclusions.

70. Some examples of this lack of explanation are the following:

P 3 Shilson Report: "o Mr. La Place held other cryptocurrencies on April 1st, 2017. … ■ It is my professional assessment that Mr. La Place likely has other undisclosed holdings of other cryptocurrencies, held on or before April 1st, 2017, based upon a multitude of reasons outlined throughout this report".

71. This raises the questions:
- How was the cited 'professional assessment' carried out, by what methodology, using what data and documentary evidence, employing what professional techniques and reasoning?
- Given that the conclusion of this 'professional assessment' is given in terms only of a vaguely-postulated 'likely… holdings', what is the strength or degree of certainty of that likelihood, and what could be the range of conclusions, with other likelihoods (if any), reasonably derivable from this 'professional assessment'?
- Which of the vaguely-stated 'multitude of reasons outlined throughout this report' are here alluded to, and where precisely in the Shilson Report are those multitudinous reasons to be found 'outlined'?

72. P 8 Shilson Report, where, beneath a 'spidery' graphic diagram (which itself is not explained – I return to such graphic diagrams later herein), RAS states:

"The above demonstrates numerous inbound transactions to a wallet cluster owned by Mr. La Place, evidently from a mixer. This was identified via following a blockchain trail from a Poloniex withdrawal. The origin of the mixed funds would be of high interest for this case".

73. The aspects of this statement which need explanation clearly include:
- How does this unexplained graphic diagram 'demonstrate' numerous 'inbound transactions' to a 'wallet cluster'?
- Even if that is what the graphic does indeed 'demonstrate', how does it prove or validate that 'a wallet cluster' (which?) is or was 'owned by Mr. La Place'?
- Even if that is what it does indeed 'demonstrate', how is it 'evident' that 'numerous inbound transactions' were 'from a mixer'? Which 'numerous' transactions – all of them? Which mixer? If not all of them, then what happened to the remainder?
- How exactly was this 'identified'? The vague and imprecise expression 'via following a blockchain trail' means little and needs clearly explaining.
- Which 'Poloniex withdrawal'? There is no reference given to any case (or other) document in which the existence of this 'withdrawal' was discovered, and from which whatever associated data RAS used has been extracted.
- Is the vague expression 'the mixed funds' intended here to be a hypothetical proposal, or are there specific 'mixed funds' being referred to? If the latter, details should be given.
- Why would the 'origin' of 'the mixed funds' be 'of interest' for this case? Is this vague statement intended as a hypothetical proposal or are there specific reasons proposed, that should properly concern an expert witness instructed in this case, as to why this should or could be 'of interest', if so, what are those proposed reasons?

74. P 11 Shilson Report: "Ox03f955aD67D0027EOBaF3DccC3dlfB5X665E61X9 was the source of this funds [*sic*] … the activity of this wallet resembles activity I would expect of an individual user. I assess it is likely this wallet belongs to Mr. La Place".

75. The questions raised here include:
- By what reasoning does this 'wallet activity' come to be assessed as that which RAS 'would expect of an individual user'?
- On what grounds and through what process does RAS 'assess' that it is 'likely this wallet belongs to Mr. La Place'?

76. P 8 Shilson Report, Footnote No 9: "*See*: Attachment-- Graph_La Place"; and P 12 Shilson Report, Footnote No 14: "*See:* Attachment: La Place FCT transactions". I have been unable to find any such Attachments to the Shilson Report.

77. P 13 Shilson Report: "It is my assessment that Mr. La Place's reasoning for procurement of Monero were one or both of the following: …
2. Mr. La Place may have wanted to keep a portion of his cryptocurrency holdings in something often described as an 'untraceable' asset".

78. Explanations of the following are needed:
- How has RAS done his 'assessment', and where was there disclosed information pertaining to or revealing 'Mr. La Place's reasoning' in order to assess such reasoning?
- Use of 'may' requires some indication of the strength of the likelihood that 'Mr. La Place may have wanted to keep a portion…' as assessed.
- Where and by whom is this 'often described as an 'untraceable' asset'?

79. P 15 Shilson Report: "Mr. La Place likely didn't become a security expert in a year".

80. Questions raised here are:
- By what assessment did RAS conclude that RLP becoming a 'security expert' in a year was unlikely?
- How or where did or does RAS define a 'security expert'?
- Is RAS actually qualified to judge whether or not RLP was or became a 'security expert'? If RAS asserts that he is so qualified, such qualifications should be given.

'blockchain forensics'

81. At P 4 Shilson Report there is the only substantive mention of an analytical tool, technique or methodology that I have been able to find reported as having been employed by RAS to carry out his instructions "to perform an analysis of cryptocurrency holdings", and it is made clear that the scope of the analyses undertaken using this tool, which is given as 'blockchain forensics', but not further explained, has been necessarily limited:
"Note, the above constitutes *only* what has been identified based upon blockchain forensics made possible thus far".

82. The term 'forensics' appears a further three times:

P 9 Shilson Report: "The BTC blockchain forensics trail for Mr. La Place's known wallets presents an extensive area of potential future exploration even with existing data, however, due to potential false positives and false attribution, only wallets that were assessed as likely to be owned and operated by Mr. La Place were included in this assessment".

P 11 Shilson Report: "Due to a lack of deposits or withdrawals for Ethereum, no forensics on this blockchain … are presented as possible".

P 11 Shilson Report: "Based upon existing discovery and disclosures, we are unable to conduct forensics on this blockchain".

83. It will readily be seen that all of the above three instances report 'forensics' that were *not* done, or *could not (completely) be done*, by RAS, and in any event the passages do not add anything in terms of defining or explaining exactly what is intended to be meant or constituted by the term 'blockchain forensics' in the Shilson Report. To the best of my experience, knowledge and belief, in the field of my expertise, computer software, systems and technology, the term 'blockchain forensics' is not a settled Term of Art, nor a defined International Standard, nor a specific proprietary name, brand or other recognisable or protected descriptor for a particular software product or package, or other tool, toolset, application, technique, protocol or methodology.

84. In my view and experience the terminology 'blockchain forensics' is merely a broad phrase describing a range of detailed technical activities that may be carried out to examine (possibly latent, or hidden) *blockchain* data, software, operations, systems, networks, records etc for *forensic purposes*, i.e. for the purposes of legal examination, usually in regard to disputes, to standards of legal evidence and procedure set down in the public justice (or Alternative Dispute Resolution) system, often in the context of a court trial.

85. There is also the, similarly generic, term 'data forensics' (and/or the even more general 'digital forensics'), with which 'blockchain forensics' is related. However, the term 'data forensics' encompasses technical and other activities carried out in retrieving, analysing, recovering, authenticating etc datasets or data records, where the data (and 'metadata') may occur on, in and among a wide range of media, systems, networks, applications, situations and scenarios well beyond those centered on or associated simply with a blockchain application.

86. A definition found readily in just one online link chosen at random accords with the understanding of the generic term 'blockchain forensics' that I have explained above:

https://www.decentralize.africa/blockchain-forensics-explained/

"*The American Heritage Dictionary defines forensics as 'the use of science and technology to investigate and establish facts in criminal or civil courts of law'. In other words, forensics deals primarily with the recovery and analysis of latent evidence. Latent evidence can take the form of fingerprints left on a window, to logs recovered from a damaged computer system or ledger transaction activities on a blockchain. Digital forensics is a growing field that implore the use of technology and other sophisticated tools…*"

87. (I note as an aside that the generalised terminology 'blockchain forensics', 'data forensics', and 'digital forensics' are not the same as the proprietary name *Forensic Systems Analysis*, which I own, together with the domain *ForensicSystemsAnalysis.com*, for a range of specific methodologies and techniques that I have developed over the past 30+ years to examine and analyse failed, stalled or faulty software, and software projects, which includes *inter alia* a definition, and objective protocol for determining, a *software material defect*, now well accepted by courts in several jurisdictions. See '*Forensic Systems Analysis: A Methodology for Assessment and Avoidance of IT Disasters and Disputes*', issued as a *Cutter Consortium Executive Report*, Enterprise Risk Management & Governance Advisory Service series, Vol. 3, No. 2, March 8, 2006).

88. It follows that the information in the Shilson Report that the analyses undertaken by RAS was through techniques or tools or whatever else based on 'blockchain forensics' does not provide any details of exactly what these were, nor precisely what was done. In my view and experience the specific tools and techniques, processes, steps, calculations, manipulations etc are almost certainly to have involved *software*. On that premise, obvious questions necessarily follow, including: which software, whose software, how was it used, was it properly used, with what data, with what operational guidance, definition, specification, and where is the working, and results obtained from the executable software?

89. I surmise that a clue to the answers may be in information on the RAS website:
https://RASXXX.com/expert-witness-testimony-on-blockchain-bitcoin-cryptocurrencies/
"*Renowned expert in blockchain forensics (utilizing tools such as Chainalysis, CipherTrace, Blockseer, or tools developed internally by request,) …*".

90. I surmise also that it may be that one or other of the tools cited there includes the means for generating the several 'spidery' graphic diagrams to be found in the Shilson Report (four of them, on P 5, P 6, P 8, and P 10), plus an explanation of the methodology of their generation, and guidance as to their meaning and interpretation. Unless I have misunderstood the way they have been presented, I can discern no explanation or assistance with their interpretation within the Shilson Report itself, nor therefore what insight they are intended to provide.

91. However, leaving aside these surmises, none of these questions concerning the software or whatever else used to carry out 'blockchain forensics' are answered in the Shilson Report. Absent such information, giving the relevant details, it is impossible for anyone, in particular another expert, to 'check the workings' of RAS, to revisit the analyses RAS carried out, and to see whether or not his results and conclusions can be confirmed.

92. I note that at P 19 Shilson Report there is the only a reference that I have been able to find to 'software methodologies'. However, in the context in which that expression is used, in one of many speculative comments, RAS does not appear to be referring there to any software or methodologies RAS has himself employed in carrying out his analyses within the Shilson Report:
"c. Mr. La Place likely has an Ethereum software wallet (such as MetaMask, MyCrypto, or MyEtherWallet) or hardware wallet (such as a Trezor or Ledger, but which are accessed via the software methodologies prior listed.)".

93. RAS does disclose another – 'blockchain forensics'-related – technical investigative technique upon which he has relied: what he describes as the 'immutable truth of the blockchain'. At P 21 Shilson Report RAS notes "… actions … are publicly presented on the blockchain in immutable and permanent truth"; and "the immutable truth presented by the blockchain". Whether or not, and to what extent may be relevant in the context of this case, this asserted 'immutability' can always be scientifically, and pertinently, a 'truth', and/or universally and at all times relied upon, I repeat that the Shilson Report in my view and experience should anyway, as a matter of standard good practice, have provided full details of the 'blockchain forensics', and/or other software and analytical tools, that were employed and relied upon to reach the conclusions and opinions presented therein.

94. Finally, RAS makes many references to a 'cluster' and 'wallet cluster' in the Shilson Report, and he endeavours to explain what he means by this terminology, at P 8 Shilson Report, Footnote No 10: "A wallet cluster includes two or more Bitcoin addresses that are clustered based upon heuristics such as cospending".

95. In my view however this does not advance understanding of a 'wallet cluster' very far: it is unclear what particular 'heuristics' RAS has in mind, or relies upon, and the jargon 'cospending', which as far as I am aware is not an English word, needs defining and explaining as to what he intended it, in context, to mean.

'wallet monitoring notifications'

96. At P 4 Shilson Report RAS discloses that:
"It is also worth including that any wallets identified as presently having balance have had wallet monitoring notifications enabled for them, rendering any activity (regardless of whether inbound or outbound in nature) to automatically result in a notification. In the event Mr. La Place initiates transactions of any identified dormant funds, I will be aware of such transactions taking place".

97. In my view and experience this raises troubling concerns about the Shilson Report, and about the professionalism and standards of the methodologies and expert investigative approach employed by, and aspired to, by RAS in the conduct of his analyses. In particular, the questions raised are:

(1) Has RAS taken, or did anyone in the Plaintiff's legal or expert team take, a *forensic image* of all of the datasets and software upon which the Shilson Report relies, as at a recorded and authenticated date, so that standard 'Chain of Custody' can be established, preserved and proven, where the forensic image (whether or not held in secure escrow) can *inter alia* at any point be validated, and checked-against, to allay any concern later arising that evidence may have been tampered with?

(2)   RAS here discloses that he himself has already made changes to the operational configuration or status of a wallet or wallets whose data may, by his own admission, be, or become, evidence in this case, saying that "wallets … have had wallet monitoring notifications enabled for them. In the event Mr. La Place initiates transactions … I will be aware of such transactions taking place". If RAS sought and obtained the consent of RLP to carry out this transaction surveillance upon wallets that RLP may own or use, by way of such wallet-monitoring 'notification enablement', then it may be that no issue arises. However, if that permission was not sought by RAS, nor given by RLP, then I consider that a key question is: by what authority did RAS, on his own initiative and responsibility, make these changes to evidence for what he discloses are his own 'transaction awareness' purposes?

4.2.6 Analysis of cryptocurrency transactions presented in the Shilson Report

98.   As I have emphasised above, in the absence of any material and substantive information in the Shilson Report as to the identification and details of the 'blockchain forensics' software and/or all other software and analytical tools used by RAS to arrive at and present his results therein, it is impossible independently to check, where need be, his technical discourses concerning the "analysis of cryptocurrency holdings of Roderick J. La Place" that he has carried out.

99. Even leaving that fundamental difficulty to one side, given the limited time, effort and budget that I have had available to work on production of this my **Expert's Report**, it has not been possible for me to begin to undertake examinations that would include carrying out my own technical investigation or research on or into all the specific or detailed 'blockchain forensics', cryptocurrency trading, wallet etc instances referred to within the Shilson Report, and, as I have made clear at the outset, this level of detailed technical investigation was not within the scope of my instructions.

100. However, I have endeavoured to address a few instances of the findings presented in the Shilson Report concerning specific cryptocurrency transactions analysed by RAS.

101.   I first note that RLP himself appears to have been definite and sure about certain aspects of the numbers of holdings, and related matters, in his sworn deposition evidence, taken on Thursday, January 25, 2018:

P 15 DEPOSITION OF RLP:
Q: "… you have never converted any of the bitcoin that you purchased back into cash, is that correct?".
A: "**That is correct.**".

P 16 DEPOSITION OF RLP:

Q: "What about wallets?".
A: "**What do you mean?**".
Q: "Do you have any wallets with Coinbase?".
A: "**No.**".
Q: "Do you have any wallets with Poloniex?".
A: "**No.**".

P 16-17 DEPOSITION OF RLP:
Q: "Okay. Do you have any external thumb drives?".
A: "**All right. I -- back up. Coinbase does have wallets associated with it. It's a vault to wallet transaction to – yeah, so they have. I was thinking that was part of the core protocol. I was thinking like a third-party wallet tied to them. Poloniex does not have wallets.**".

P 24-25 DEPOSITION OF RLP:
Q: "… do you have any connection with bitcoin that would make them want to modify whatever they are reporting and their information that they are providing? Do you have any connection with them?".
A: "**I don't understand the question.**".
Q: "Are you affiliated with them in such a way that they might be influenced by you to modify any of their records?".
A: "**Bitcoin is not a company. It's not an entity. It's just a network protocol.**".

P 25-26 DEPOSITION OF RLP:
Q: "Do you stand by the assertion in court that you only had 37 bitcoin total at the time of --".
A: "**27.**".
Q: "27?".
A: "**27.**".
Q: "27 bitcoin total at the time of the divorce?".
A: "**That was the appropriate assumption of personal community property at the time, yes.**".

102. The Shilson Report appears not to have considered that the explanations given and positions described by RLP may have been, and be, essentially accurate, and thus worked even-handedly on the basis of examining whether that could indeed be confirmed (in whole or in part). To the contrary, a stance for the examinations carried out by RAS appears to have been taken on the basis of possibly pre-judging negatively RLP's 'honesty' (see P 21 Shilson Report) and proceeding with performing "an analysis of cryptocurrency holdings of Roderick J. La Place" on that potentially antagonistically biased basis.

103. I have briefly been in contact direct with RLP and have been able to take account of comments he has given to me concerning and in places rebutting the analyses of certain transactions presented in the Shilson Report, as follows.

1) A first overall observation is that I believe RLP broadly accepts that essentially all the entries in the Coinbase and Poloniex documents are accurate as to trading activity undertaken by RLP, albeit his position, as I understand it, is that he was generally "acting as Trustee for Trust assets". RAS appears to have completely omitted any consideration as to the status of the transactions he has analysed in the Shilson Report in terms of on whose behalf they were carried out and/or who was to have been/is to be the beneficiary of any profits/losses, growth/decrease in asset values etc arising from such transactions. This may be understandable: in my view and experience, I can see that in the instruction to RAS to "perform an analysis of cryptocurrency holdings of Roderick J. La Place", the word 'of' could easily be taken, either by design or accident, not to be a request to distinguish between holdings held on trust from those held for 'own account'.

2) P 5 to P 8 Shilson Report, beginning with:
"Mr. La Place withdraws 2 Bitcoin from Coinbase in transaction 41fe93c6fc023bl49417d24b875dxb6cf3552t7c940t73ced6ea9ae32x010386."; ending with:
"… numerous inbound transactions to a wallet cluster owned by Mr. La Place, evidently from a mixer".
I am assured by RLP that he has never used a 'mixer' and does not know how to do so. I have already raised the point, earlier in this **Expert's Report**, that RAS does not explain how or why he asserts that it is it 'evident' that 'numerous inbound transactions' were 'from a mixer'. Absent such explanation, in my view and experience the assurance given by RLP is no less reliable than the unsupported 'mixer' assertion by RAS. Furthermore, it seems to me not only that RLP's assurance could be practically tested, but that both positions could simultaneously be technically possible. In any event, RAS does not say why whether or not inbound transactions were from a mixer to a wallet cluster owned by RLP is of any relevance to the issues in this *La Place v La Place* case.

3) P 11 Shilson Report, paragraph beginning:
"Wallet 0x03f955aD67D0027E0BaF3DccC3dlfB5X665E61X9 bas extensive utilization of varied ERC-20 tokens, which fits a theory I initially held about Mr. La Place's cryptocurrency dealings (involvement with ICOs and altcoins) early on while writing this report. The wallet transacts over 16,790 ETH historically, has a present balance of 65.577 ETH …".

104. RLP informs me that he has no idea of what is being referred to in this paragraph, confirming that he has traded in and out of ETH, but nowhere near 16,790 ETH. He furthermore has no knowledge of who some of these addresses belong to, since he traded online and peer-to-peer ('P2P'), without knowing names.

105. Once again, RAS introduces vague and incomplete information, referring to a 'theory I initially held about Mr. La Place's cryptocurrency dealings'. In this RAS notes an unspecified '(involvement with ICOs and altcoins)', 'early on while writing this report', without providing any details as to what that theory is (or was), its grounding and provenance, whether or not RAS still held to that 'initial' theory by the time he had finished writing the Shilson Report, and what, if anything, that undisclosed theory had or has to do (if anything) with leading to his asserted quantified conclusion that 'The wallet transacts over 16,790 ETH historically'.

4) P 3 Shilson Report, paragraph beginning: "• $2,213,666.752 worth of cryptocurrency was withdrawn from Poloniex between August 11th, 2016 and November 8th, 2017".

106.   RLP avers to me that he "cannot verify $ amounts of crypto at a point in time": this is understandable in my view (see my exposition on valuation of digital assets earlier in this my **Expert's Report**). Furthermore RAS does not explain why he is using USD valuations (and not cryptocurrency-denominated values), and selecting the particular date that he has picked. This would seem to be all the more puzzling in that RLP assures me that "no trade was ever made back into USD".

5) P 5 Shilson Report: "Mr. La Place had a whitelisted wallet on Poloniex which sends funds to Bitcoin wallet 14k7PtWxxSx2qZ9JSxc3yf2bwsNsseYrKz. Wallets in this cluster have received approximately $1,074,665.675 and this wallet currently holds 250.004 BTC".

107.   RLP notes that a review on any public block explorer, such as at btc.com, clearly shows that this is not accurate, and I have checked that this is indeed as RLP says:
https://btc.com/14k7PtWxxSx2qZ9JSxc3yf2bwsNsseYrKz
Total Received 80.19238166 BTC
Balance 79.44238166 BTC

108.   As I have made clear, in the limited time that I have had available for my work, it has not been possible for me to begin to undertake examinations that would include carrying out my own technical investigation or research on or into all the specific analyses of the Shilson Report. However, given the above large discrepancy, in this one transaction in the Shilson Report, where the figure of 250.004 BTC reported by RAS as held by the wallet is over **three times** the actual current balance recorded of 79.442 BTC, I have to express concern that such gross misreporting by RAS could possibly be replicated throughout the Shilson Report, and, if so, in my view a legitimate conclusion could be that the RAS analyses – however they have been carried out – cannot be wholly, if at all, relied upon.

6) P 22 Shilson Report: "over 287 BTC was withdrawn from Poloniex prior to April 1st of 2017. After April 1st, 2017, Mr. La Place withdrew over 459 BTC from his Poloniex account".

109.   RLP notes to me that this figure of '459 BTC', too, is incorrect and that "the records show it to be approximately 354 BTC". He also informs that he has copies of a 'personal' wallet and 'Trust' wallet that he says clearly show the funds merely "more or less going back and forth"; and he has also researched the Coinbase information from their subpoena which shows a total of 264 BTC purchased from 2015 through 2016. I have had insufficient time to be able to check this at the time of concluding the work on this my **Expert's Report**; however, I have no reason to doubt what RLP tells me, given also that, since RAS has it appears made one mistake in what he has reported in the Shilson Report, as immediately in 5) above, it seems to me that it is certainly feasible that RAS has made others.

5.   Conclusions and Opinions

110. I have carried out my instructions to
- Review the Shilson Report together with consideration of the case documentation provided;
- Produce a high-level critique of the Shilson Report; and
- Provide an introduction to the blockchain and cryptocurrency, crypto assets etc field to assist the understanding of the Court;

and my conclusions and opinions are as follows.

111. I have provided an introduction to and explanation of blockchain and cryptocurrency in general, and Bitcoin in particular, in ***Addendum A*: Introduction to Blockchain and Cryptocurrency** of this **Expert's Report**.

112.   On the basis of my review and analysis of the Shilson Report together with consideration of case documentation provided to me:

1) There is doubt as to whether or not RAS has personally carried out or directed all work undertaken in regard to his investigations, analyses and findings, and as to confirmation that the conclusions and opinions expressed in the Shilson Report are entirely his own.

2) RAS has failed to make clear in the Shilson Report on what evidence, drawn from the case documents, he relies for the analyses he carries out, and the results thereof.

3) RAS has failed to disclose in the Shilson Report what (proprietary or other) 'blockchain forensics' software, tools or techniques he has used to undertake his analyses and arrive at his conclusions.

4) RAS presents 'spidery' graphic diagrams in the Shilson Report that appear to have been constructed utilising (proprietary or other) software, tools or techniques, identification and details of which RAS has failed to disclose.

5) The 'spidery' graphic diagrams that RAS presents are difficult, if not impossible, to understand or interpret as RAS has failed to give any explanatory or walk-though text within the Shilson Report to describe them, or their intended meaning or relevance.

6) A proportion of the Shilson Report is concerned with giving comments about valuations of various transactions in USD which valuations are in my view outside the scope of the 'analysis of cryptocurrency holdings' which he says he was asked to carry out.

7) A further proportion of the Shilson Report is concerned with giving comments and making insinuations about potential criminality of the actions of RLP which are also in my view outside the scope of the 'analysis of cryptocurrency holdings' which he says he was asked to carry out.

113. In summary, it is my opinion that the Shilson Report is essentially unreliable. Not only is some 63%, in total, of its content, in my view, out of scope as regards the instructions to RAS, and/or out of line with an expert's overriding duty to the Court, but it also largely fails to provide 'an analysis of cryptocurrency holdings of Roderick J. La Place', as requested of RAS, that is capable of being easily understood, if at all, as to the basis upon which RAS arrives at his results, and/or the identification, validity and veracity of the software, forensic methods and technical processes employed to derive his results, and/or the nature and quantification of the results themselves.

114. In my opinion the Shilson Report sets out neither the evidence upon which it relies, drawn from the case documents, nor the principles and detailed technical processes by which analyses of that evidence have been carried out, nor the rationale for arriving at its findings, conclusions and opinions, in any credible or rigorous way capable of being revisited and/or checked by another expert.

115. In the time available for production of this **Expert's Report**, it has not been possible for me to undertake examinations that would include carrying out my own technical investigation or research on or into all the specific or detailed 'blockchain forensics', cryptocurrency trading, wallet etc instances referred to within the Shilson Report, and, as I have made clear at the outset, this level of detailed technical investigation was not within the scope of my instructions. However, I have addressed a few instances of the findings presented in the Shilson Report concerning specific cryptocurrency transactions and have discovered what appears to be a large discrepancy in one transaction therein, where the figure of 250.004 BTC reported by RAS as held by a wallet is over **three times** the actual current balance recorded of 79.442 BTC. It is possible that such gross misreporting by RAS could be replicated throughout the Shilson Report, and, if so, in my view the RAS analyses and quantifications of cryptocurrency holdings cannot be relied upon.

116. In terms of the principal technical issue that I have ventured to surmise RAS might have implicitly been instructed to address, my opinions are:

> The Issue for Experts
> Based on the documents provided and evidence disclosed in the case:
> (i) What were, at a defined date, or dates, the cryptocurrency holdings of Roderick J. La Place. <u>My opinion</u>: the Shilson Report has failed to identify and/or quantify clearly any cryptocurrency holdings beyond those that were, and are, not contested by RLP.
> (ii) Where are these crypto assets held today. <u>My opinion</u>: the Shilson Report has failed to provide clearly any further information beyond that not contested by RLP.
> (iii) What are the technical processes or protocols through and by which such crypto assets would be accessible and potentially realizable in US Dollars or other fiat currency. <u>My opinion</u>: despite presenting discourse on many individual cryptocurrency transactions, accompanied by proprietary 'spidery' graphic diagrams whose possible insights (if any) are largely unexplained, the Shilson Report has omitted to answer this.

6.   Appendices

Appendix ONE: Dr Stephen Castell – qualifications and experience

Management, Financial and Business Development Consultant in Information Systems,
Computer and Communications Software, Technologies, Industries, Legislation and Regulation, Broadcasting,
Media, Telecommunications, Internet, E-commerce.   New Entrepreneurial Business Development Specialist.
Expert Witness. CEDR-Trained Mediator, ICC Arbitrator, Expert Determiner.
On the List of Experts: Arbitration and Mediation Center, *World Intellectual Property Organization*, Geneva
Analytical ● Creative ● Practical ● Professional

Education

> University of Nottingham
> PhD in Mathematics : "*Certain Transformations in Gas- and Magnetogas- Dynamics*".
> Whole PhD thesis published in international mathematics/physics journals.   Postgraduate Prizewinner.
> MSc in Mathematics (Computer Science and Fluid Mechanics)
> University of London
> BSc First Class Honours in Mathematics, Physics and Psychology
> Schooling
> Hamond's Grammar School, Swaffham, Norfolk
> 11 'O' Levels, 2 'A' Levels.   House Captain.   Athletics *Victor Ludorum*.
> Prince Rupert School, Wilhelmshaven, Germany   Magnus Grammar School, Newark, Notts.

Career

1978 to present: Chairman, Castell Computer and Systems Telecommunications Ltd
('*CASTELL*' or '*CASTELL Consulting*')

> Own independent consultancy company.   *CASTELL* specialises in the strategising, planning,
> management and development of businesses in information and communications technologies,
> broadcasting and the media, and in analysing and influencing the financial, market, economic,
> regulatory and legal factors which affect them. It undertakes professional consultancy in IT and
> communications software/systems development, management and strategy.   Dr Castell is in
> particular well known for the high quality and effectiveness of his work as an Expert Witness in
> major computer software and systems litigation having developed powerful techniques of
> *Forensic Systems Analysis*, and having achieved a special reputation in researching computer law
> and evidence issues.   He has a track-record for business development/management in the fields
> of professional services, e-commerce/the internet, new media, databroadcasting, satellite, digital
> television, and image, voice, data and multimedia communications, particularly for entrepreneurial
> new companies and corporate venturing.

Previously: ● Manager, Group Management Services
> Bremar Holdings Ltd, international merchant bankers
> ● Consultant, Touche Ross & Co, Management Consultancy
> ● Senior Mathematician, Bearing Research Centre, RHP plc
> ● Applied Mathematician, Chalfont Park Research Laboratories, BACo plc.

Publications

A large number of papers and articles in national, international, professional, trade and technical press on IT,
mathematical, technology, finance and investment subjects. Bestseller book "*Computer Bluff*", 1983. "*The
APPEAL Report*", May 1990, a major study commissioned by the CCTA (H M Treasury) on admissibility of
computer evidence in court and the legal reliability/security of IT systems. Numerous letters published in e.g.
The Times and *Financial Times* on business, finance, technology, communications, science and law topics.
Many appearances at International Conferences to present papers on e.g. information services, software,
databroadcasting, satellite business services, digital television, computer evidence, venture capital, enterprise
management, litigation and ADR. Author and Presenter of '*Avoiding IT Disasters – the Expert Way*' Course,
first held Nice, France, March 2005. His seminal 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). Author of
the much-cited '*The future decisions of RoboJudge HHJ Arthur Ian Blockchain: Dread, delight or derision?*',
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.

Other Qualifications   **Languages**

CITP, Chartered IT Professional

FIMA, MInstP, MBCS, MCMI, CPhys, MIoD   Working knowledge of French and German

MEWI, Member of the Expert Witness Institute

Law Society's Directory of Expert Witnesses

Awards and Recognitions

Medallist, *IT CONSULTANT OF THE YEAR,* British Computer Society IT Professional Awards, 2004.

Corporate America News Expert Witness of the Year 2016 (Risk Assessment & Management).

Computers Expert Witness of the Year (*Lawyer Monthly*), Expert Witness Awards 2016.

2019: Honoured with an interview for *Archives of IT: Capturing the Past, Inspiring the Future*

In-depth experiences of the people who influenced the development of IT in the UK:

https://archivesit.org.uk/interviews/stephen-castell/

Recreations

Business, Family. Swimming, Music, Sailing, Tennis. Patron, *London Cantamus Bach Choir and Orchestra*.

Past Parent School Governor, 1982-1985. Endowed "*Castell Computer Creativity Contest*".

Committee Member, British Computer Society (BCS) *Law Specialist Group*.

Member, Real Time Club. Past Member, Working Groups of BCS Strategy Review Panel.

Past Member, BCS *Legal Affairs Committee*.

Past Correspondent Panel Member, *Computer Law and Security Report* (now *Review*), Elsevier.

*CASTELL Consulting***'s clients have included:**

Airtours plc (Expert Witness in its action *versus* EDS)

Axon Solutions Ltd (Expert Witness on behalf of *Hiscox*, its PI Insurers, in re its position as Part 20 Defendant in the *W H Smith versus Fujitsu Siemens Computers* action concerning UK's largest SAP implementation)

British Broadcasting Corporation (BBC Data; Telecoms/Broadcasting Regulatory & Business Strategy)

BBC Enterprises Ltd (BBC Datacast; BBC Eurocast/OLYMPUS Satellite)

British Telecom plc (New Venture Business Development; Satellite Services)

BT Syntegra (Expert Witness in its actions *versus* Ministry of Defence; and SwapsWire)

Cable and Satellite Telecomms. Ltd (National Transcommunications Privatisation; Channel 5 TV Licence Bid)

Central Computer and Telecommunications Agency (CCTA, H M Treasury, British Government)

Cincinnati Bell Information Systems Ltd (Cable TV/Telephony Systems and Services)

Department of Trade and Industry, British Government (Telecoms Product Development; VANS Licensing)

European Commission/BT Tallis (INFOSEC Trusted Third Party Services)

European Space Agency (Satellite Databroadcasting) France Telecom (New Venture Advice; AT&T Telemarketing)

GEC-Marconi (Expert Witness in its action *versus* London Fire and Civil Defence Authority)

H M Treasury (Expert Witness - Lord Chancellor's Department in its action *versus* Price Waterhouse)

HSR, Milan (Expert Witness in its action *v.* ACT Medisys re Hospital IS for large Italian Hospital)

International Chamber of Commerce, Paris (Arbitrator in 3-man ICC Arbitral Tribunal, European litigants)

INFOCAST/Citibank (Databroadcasting Strategy)

London Ambulance Service (Expert Witness in its action *versus* CAP-CGS)

Mercury Communications Limited (National Transcommunications Privatisation)

Misys plc (Expert Witness on major cases in the UK, Italy, Ireland, Australia; Business/Product Strategies)

Motorola (Mobile Communications Interconnect and Licensing)

Pearson Group plc/Financial Times (Databroadcasting Strategy)

Personal Communications Networks: Mercury PCN and Unitel

SAIT Electronics SA, Belgium (Satellite Communications and Databroadcasting Development)

Superdrug Stores Plc (Expert Witness in its actions *versus* TEC UK Ltd)

The Meteorological Office, UK (New Business Development: Data/Databroadcasting Services)

The Press Association, London (Satellite Data Distribution).

Transfield Obayashi Joint Venture (Expert re Australia's largest infrastructure project, *Melbourne Citylink*)

United Arab Shipping Company S.A.G., Kuwait (Expert Witness in software action *v.* BIDM, Inc, New York)

Links   http://www.castellconsulting.com/

http://www.e-expertwitness.com

http://www.computerweekly.com/Articles/2005/09/13/211761/Disasterbutnorecovery.htm.

Appendix TWO: Documents Provided and Reviewed in this Report

1. Received on October 09th, 2020, from *Roberts Stoffel Family Law Group*, in separate pdf files as follows:

Document ID	Total Pages
Pdf file name: 'Plt's 2nd supp disc 052920 LA PLACE.pdf'	28
PLAINTIFF'S 2ND SUPPLEMENTAL POST DECREE DISCLOSURE OF WITNESSES AND DOCUMENTS PURSUANT TO NRCP 16.2 29th day of May, 2020	5
Shilson Report	23
Pdf file name: 'Documents for Dr Castell 100920 pursuant to correspondence.pdf'	240
ORDER FREEZING ASSETS	2
SUBPOENA DUCES TECUM TO COINBASE	12
CLP'S SUPPLEMENTAL PRODUCTION	3
Letter from Coinbase June 18-2018	3
Coinbase Account Statement 1: 01/23/2015-03/23/2018	8
Coinbase Account Statement 2: 02/16/2015-07/25/2018	2
Coinbase Account Statement 3: 06/01/2016-07/25/2018	1
Letter from Carter [Poloniex] January 12-2018	1
Poloniex Statement - 'Entity 99NNN Account #100NNNNN'	53
Poloniex KYC ID for RLP	2
Poloniex DECLARATION OF CUSTODIAN OF RECORDS	1
CLP'S PRODUCTION OF DOCUMENTS	79
DEPOSITION OF RLP	37
CLP'S FIRST INTERROGATORIES TO RLP	5
CLP'S REQUESTS FOR ADMISSIONS TO RLP	3
CLP'S FIRST REQUEST FOR PRODUCTION OF DOCUMENTS TO RLP	2
SUBPOENA TO COINBASE	5
SUBPOENA TO POLONIEX	5

2. As I initially read through the second of these pdf files, the 240-page 'Documents for Dr Castell 100920 pursuant to correspondence.pdf', I made brief summaries and notes, for ease of future reference and analysis. These are in the separate document 'Contents of Documents for Dr Castell 100920 from Attorney Roberts 19Oct2020.pdf'.

Appendix THREE: Qualifications and experience of Mr Robin A Shilson

'Robin-Shilson-expert-witness-cv.pdf':   separate   document,   downloaded   from
https://RASXXX.com/expert-witness-testimony-on-blockchain-bitcoin-cryptocurrencies/
Curriculum Vitae of Robin Shilson

> *Summary: a blockchain forensics expert and cryptocurrency cybercrime investigator with experience in dozens of cases. Seen as subject matter expert by law enforcement and regulators. Experience working with multiple law firms performing forensics work and other expertise-based supportive efforts. Experience testifying and writing Declarations for numerous cases involving cryptocurrency, including OTC deals and simswaps.*

RASXXX Co-Founder/CSO

> ● *Renowned expert in blockchain forensics (utilizing tools such as Chainalysis, CipherTrace, Blockseer, or tools developed internally by request,) briefing law enforcement, legal professionals, and senior level exchange executives on complex blockchain transactions, security vulnerabilities, and other rapidly evolving elements of new waves of crime*
> ● *Expert witness with experience leveraging deep knowledge of cryptocurrency criminal methodologies and Networks …*

https://www.almexperts.com/expertsbio/Robin-Shilson-RASXXX
Robin Shilson, RASXXX
www.RASXXX.com

https://RASXXX.com/expert-witness-testimony-on-blockchain-bitcoin-cryptocurrencies/
If you are looking for an expert witness who can explain the facts about blockchain-based digital assets, renowned industry thought leader Robin Shilson is the man for you. Robin has extensive experience "writing the book" on mapping blockchain transactions and explaining the movement of assets to laymen with little or no blockchain experience in a way that simply makes sense, with meticulously constructed graphics to illustrate typically hard-to-understand flows in an easily interpreted way. Robin is seen as a subject-matter expert by the FBI and for Special Agents who have questions concerning blockchain-related cybercrime. Robin prides himself on a very strong working relationship with the FBI and sees the opportunity to help law enforcement and the government with this new technology as a blessing. Robin has consulted for numerous blockchain projects on optimizing their security posture, preventing the potential loss of millions of dollars worth of assets. He has also assisted in the development of procedures for major exchanges, regarding asset theft and policies such as the GDPR.

https://www.youtube.com/watch?v=KnvtxYo95XX
Discussing RASXXX With Robin Shilson | 22 May 2019 Stan Cutting

> *I interviewed Robin Shilson who is the founder of RASXXX, one of the only blockchain investigation agencies. They have recovered millions of dollars of stolen funds, prevented dozens of ICO scams, and professionally handled PR disasters and other emergency situations.*

Some final thoughts he left us with were:

> *Continue to do your own research. If something seems too good to be true, it probably is. Things that have been business practice in other industries apply here. If you don't know the person, don't send them crypto, if you don't know where or how to report a scam or hack, don't send them your money, if you, amongst other safety tips. This must be an industry-wide effort.*

These were the questions I asked him:

> • *Can you tell us a little bit about yourself?*
> • *How busy are you now / How does your day look?*
> • *Can you give us a brief introduction to your business?*
> • *What gave you the idea and when did you start it and or begin to discuss the idea?*
> • *What's up next for RASXXX?*

> • What are some of the biggest problems you see in the industry currently?
> • What changes do you see coming to the industry over the next 1-2 years?
> • What obstacles do you see to mass adoption of blockchain technology?
> • What are your thoughts on censorship and free speech with everything that has been happening in the media and on social media?
> • How is RASXXX different from other companies in the crypto securities and investigations space?
> • Where do you see your company going in the next year? The next 5 years?
> • Can you share any interesting cases you've worked on or intriguing stories?
> • Is there anything else you'd like to say to the audience?

You can check out their site here: https://RASXXX.com/
> https://steemit.com/@RASXXX/
> https://www.facebook.com/RASXXX/
> https://twitter.com/ RAS_XXX
> https://www.linkedin.com/company/RASXXX
> https://t.me/RASXXXann
> https://medium.com/RASXXX

https://davidgerbil.co.uk/blockchain/2019/03/25/RASXXX-response-from-Robin-Shilson/

7.   *Addendum A*: Introduction to Blockchain and Cryptocurrency

Introduction and Overview

A blockchain is a digital record of transactions. The name comes from its structure, in which individual records, called blocks, are linked together in single list, called a chain. Blockchains are used for recording transactions made with cryptocurrencies, such as Bitcoin, and have many other applications.

Each transaction added to a blockchain is validated by multiple computers on the Internet. These systems, which are configured to monitor specific types of blockchain transactions, form a peer-to-peer network. They work together to ensure each transaction is valid before it is added to the blockchain. This decentralized network of computers ensures a single system cannot add invalid blocks to the chain. When a new block is added to a blockchain, it is linked to the previous block using a cryptographic hash generated from the contents of the previous block. This ensures the chain is never broken and that each block is permanently recorded. It is also intentionally difficult to alter past transactions in blockchain since all the subsequent blocks must be altered first.

While blockchain is widely known for its use in cryptocurrencies such as Bitcoin, Litecoin, and Ether, the technology has several other uses. For example, it enables 'smart contracts', software programs which execute when certain conditions are met. This can provide an automated escrow system for transactions between two parties. Blockchain can potentially be used to allow individuals to pay each other without a central clearing point, as in Automated Clearing House and wire transfers. It has potential to increase markedly the efficiency of stock trading by allowing transactions to settle almost instantly instead of requiring three or more days for each transaction to clear.

Blockchain technology can also be used for non-financial purposes. For example, the InterPlanetary File System (IFPS) uses blockchain to decentralize file storage by linking files together over the Internet. Some digital signature platforms now use blockchain to record signatures and verify documents have been digitally signed. Blockchain can also potentially be used to protect intellectual property by linking the distribution of content to the original source.

How Bitcoin really works

The question "Hey, how does it 'really work', this Bitcoin?" is often heard, and it can seem that there is considerable confusion, and possibly misinformation, on the subject.

If you could 'pick up a Bitcoin and look it over', what would you see? Well, *nothing* meets the eye—the Bitcoin is contained in something that is virtual, rather than anything physical, a *Bitcoin wallet*, essentially the equivalent of a bank account. This wallet allows Bitcoin to be received, stored, and then sent on to others. If you own Bitcoin, think of the wallet that contains it as your personal interface to the Bitcoin network, similar to how your online bank account is an interface to the regular monetary system. This wallet contains a private key, a secret code, that allows you to transfer or trade Bitcoin.

It is useful to try to straighten out further some detailed technical elements of the 'Bitcoin birth and lifecycle', and to take that a layman's step, or 'one dumb question', at a time.

1. One bitcoin is 'created', coming into someone's initial ownership: i.e. someone mines 1 bitcoin, or gets 'rewarded' with 1 bitcoin ('BTC') for 'verifying transactions'. *Yes or no, is that what happens? Or what?*

That's what everyone may be told happens. But it isn't. Every ten minutes records are taken from a backlog (the *Mempool*) and put into a block 1MB in size, around 2,000 transactions. A competition is then held for miners to calculate a *nonce*, which is a number that when added to the rest of the data in the block and cryptographically hashed gives an output of a specific format (with a certain number of leading zeroes).

The winner of this race is allocated a reward, 12.5BTC (or 6.25BTC after the 'halving' https://blockgeeks.com/guides/bitcoin-halving/). This reward is notated as the first record in the next block. So at the beginning of each block there is a transaction from 'Coinbase' for 12.5BTC going to the wallet address of the miner. This is where what happens in the real world, and what people think happens, differ. The miner is not rewarded with 1BTC, serial number 'xyz1', 1BTC serial number 'xyz2', etc. No, the miner is allocated 12.5BTC 'worth' of BTC. So it's like putting $100 in your bank account, $100 on the bank's ledger. It *isn't* a register that you own $1 serial number 'xyz1', $1 serial number 'xyz2', etc…

So, what we see on the Bitcoin Blockchain Ledger, https://www.blockchain.com/explorer, is a BTC balance created from thin air and allocated to the miner's public key (which ISN'T a wallet). Think of it as a Post Office Box Number.

2. Isn't that 1 bitcoin's 'genesis' or 'birth' recorded somewhere on a (public) blockchain? *Yes or no? Or what?*

Yes, the allocation of the 12.5BTC (or 6.25BTC) WORTH is recorded in the first transaction of the next block. That's always a good 'pub quiz question' to ask to see if someone actually knows how Bitcoin really works.

3. How is the record of that 'bitcoin birth' recorded? Is it not essentially recorded as "Mined as at <date 0> by {who?} in {where?}", and as 'one amount associated with one address, a unique string of letters and numbers' (eg 1Ez69SnzzmePmZX3WpEzMKTrcBF2gpNQ55)? *Yes or no? Or what?*

Yes, it is. For example, we can see this on https://www.blockchain.com/btc/block/0000000000000000000f938f46a145f5f85a5e956f04751367affec12128eb4d

This contains the details of block 621096, mined at 2020-03-10 15:25 by a miner known as *Slushpool*. Here's the coinbase transaction:

4. That 1 bitcoin is then sold on to a first buyer, just 1 bitcoin, 1 buyer; and that Transaction Number 1 is of course recorded on a blockchain, with data essentially of at least "Transacted as at <date 1>". *Yes, or no? Or what?*

Yes, the transfer is recorded. In fact if you go to https://www.blockchain.com/btc/block/000000000000000000f938f46a145f5f85a5e956f04751367affec12128eb4d and click on the address highlighted above you will see that transactions have subsequently transferred elsewhere. Scroll down the page and you will see an example:

Hash	0e8a76bafc9a2179c2cb9e1d98b0b7efd624…			2020-03-10 11:04
	bc1qscxza3clrcd9qag3…	2.92836949 BTC 🌐	bc1qu6eak33jwf5y5e3r…	0.01018730 BTC 🌐
	1CK6KHY6MHgYvmRQ…	12.71716448 BTC 🌐	1Hqse5scWX5wxECRSw…	0.01011556 BTC 🌐
			39M4WgVdrs1xsnBWT…	0.00108457 BTC 🌐
			16GD5oi2gzh5xmKbL2…	0.00103689 BTC 🔴
			1EWmnpyM2uj79uYpt1…	0.01009900 BTC 🌐
			38PBbTyLF2YfgYH3Qy…	0.00540305 BTC 🌐
			3PzGJRKmHG547bXLK…	0.38685691 BTC 🌐
			17AEm14WxFMEMUWL…	0.00092454 BTC 🔴
			3CzuzgHGmjihixLaqpt9…	0.01002275 BTC 🔴
			bc1qx9afa9zlzmldfls0…	0.00296369 BTC 🌐
			Load more outputs… (438 remaining)	
Fee	0.00374450 BTC (24.864 sat/B - 6.250 sat/WU - 15060 bytes)			**-12.71716448 BTC**

So it looks like this busy miner has paid out a bunch of BTC to over 400 addresses in one transaction. The challenge is that, just like money in your bank account, there is no way of knowing that any particular amount is directly from another amount (because it isn't).

5. To keep it simple, let's assume that this first new owner of that 1 bitcoin did not own any bitcoins prior to his/her purchase thereof, and after Transaction Number 1 does not add to his/her holding. This first owner now has the bitcoin essentially 'stored alone' in his/her wallet, i.e 'containing' just that same single bitcoin address "1Ez69SnzzmePmZX3WpEzMKTrcBF2gpNQ55". *Yes or no? Or what?*

Let's not mix up wallets and addresses. The Bitcoin Blockchain allocates BTC values to addresses. A wallet, whether hardware or software, simply holds details of those addresses. A wallet also usually has functionality to store public and private keys and can sign transactions, using the Elliptic Curve Digital Signature Algorithm (ECDSA https://en.bitcoin.it/wiki/Elliptic_Curve_Digital_Signature_Algorithm). If we looked at the history of that person's bitcoin address, we would indeed just see the one transaction coming in.

6. Transaction Number 2: that first owner sells that same 1 bitcoin to another person (again, to keep it simple, owning no bitcoin prior to this transaction, and none further added afterwards). This Transaction Number 2 is also recorded on a blockchain, with data essentially of at least "Transacted as at <date 1.1>". *Yes, or no? Or what?*

Yes, with same caveats as above, it shows value transfer from Address A to Address B. If you've looked at some of the transactions on the explorer you'll get this now.

7. The second owner, in turn, now has the bitcoin alone stored in his/her wallet, 'containing' just that same single bitcoin address "1Ez69SnzzmePmZX3WpEzMKTrcBF2gpNQ55". *Yes or no? Or what?*

Not quite. Remember values are stored against addresses. Wallets store addresses. Wallets don't therefore hold bitcoin, they provide the means to access them.

8. After N such simple identical sell-buy transactions we arrive at, say, Robin, owning that same 1 bitcoin, by way of Transaction Number N, "Transacted as at <date 2>"; and thus someone is then able to say, by appropriately interrogating the relevant blockchain records: This 1 bitcoin has "wallet address {XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX}. It was originally mined by {who?} in {where?}, and after being mined was transferred (bought and sold) [N] times between <date 1> and <date 2>". *Yes or no? Or what?*

No. But… We can use the Bitcoin Blockchain to see values allocated to addresses changing. So we could see that Robin had 1 BTC "worth" in his address 12345xxxxx and then a message with a transaction to "move" 0.5BTC to Stephen's address 6789xxxx took place. And we would also see the remaining 0.5BTC being sent back to Robin's address because Bitcoin uses 'unspent output from bitcoin transactions'
(UTXO https://www.investopedia.com/terms/u/utxo.asp).

This is where there can be potential befuddlement between those who regularly transact in BTC who *think* they understand how it works, versus those who *know* how it *actually* works. For example, prosecuting authorities can bring actions against crypto scammers, fraudsters and illegal users of BTC because prosecutors don't have to prove a specific BTC was used in illegal activity (think 'individual banknote' in fiat currencies). This is similar to how a drug dealer will have an entire bank account seized and not just the individual USD notes that were obtained illegally. You can track transactions between Bitcoin accounts. But the transactions are *changes in ledger balance values* and *not* movements of specific coins, albeit the latter is what it looks like to those who don't know better.

Furthermore, the ledger balances and the Bitcoin accounts could all be owned by entirely different real people or, equally, they could all simply be in the legal ownership and control of the same person – just as for USD, the same person may hold and operate several different bank accounts, and also either with the same bank, or with different banks, and move his or her own USD between them. Bitcoin value movements as tracked on the Bitcoin Blockchain and as may be recorded as changes in addresses accessed via wallets may in reality be nothing more than the digital currency equivalent of someone moving his or her own USD notes and coin 'from one pants pocket to another'.

Just as anyone could have many different (varying) piles, or pockets full, of USD notes and coins, and many different pants pockets, all of which could change with time, with no one-to-one relationship ever among them, so any one person could have many different, changing BTC values recorded on the Bitcoin Blockchain, and many different wallets recording, dynamically, their addresses.

The fundamentals of analysis of cryptocurrency and blockchain transactions

There is much in the technical literature on analysis of cryptocurrency and blockchain transactions, including in regard to identifying and verifying account holders, and associated transactions carried out by them **[1]**. To my knowledge few, if any, techniques and processes that seek to do this have achieved wide or generally-recognised standing either legally or technically.

It should be borne in mind that *blockchain* still has few settled international standards, and the concept, and device-implementation, of a *cryptocurrency wallet*, its definition, structure, meaning, interpretation and use are not wholly standardised or consistent. They are also operationally dependent on, and subject to manipulation by, wallet-specific private vendor software, which is rarely independently verified or checked as to functional correctness or adequacy, quality, reliability, consistency, security and forensic provability **[2]**.

Cryptocurrency frauds and scams routinely occur and the amounts of fiat money now relentlessly misappropriated criminally runs to many billions of USD. It is a feature of these activities that (i) they principally involve proprietary third-party transactional software and systems (eg that running and offered by cryptocurrency trading exchanges), the 'on and off ramps' that connect the trader, the end-user consumer, to the secure cryptocurrency blockchain itself: such systems may be of questionable, and unaudited, provenance, quality or reliability; and (ii) since cryptocurrency trading is essentially globally unregulated, with few checks by authorities or regulators on the *bona fides* or substantive financial standing of the promoters and operators thereof, investigators and prosecutors have difficulty identifying and/or catching perpetrators. If and when they do, they have additional challenges in securing the relevant fraudulent transactional blockchain and misappropriated crypto-asset movement evidence sufficient to prove an offence and gain a conviction to the usual 'beyond a reasonable doubt' standard.

In short, it is widely recognized that digital currencies, such as Bitcoin, readily offer convenience and security to criminals, who operate in an essentially 'black market'. And this state of affairs is unlikely to change whilst cryptocurrencies continue to exist and their trading transactions persist operationally without the backing and responsibility of Regulated/Trusted Third Parties, and thus, it has been argued, essentially outside the Rule of Law **[3]**.

For the same reason, it should be noted that investigators examining transactions and holdings of reputable and ordinary citizens who may legitimately trade and invest in cryptocurrency need to take care not to make inferences and draw conclusions of supposed illegal intent on the part of such traders and investors based only on technical analysis. Blockchain may, by virtue of its cryptographic data recording and distributed consensus mechanism, provide technically a decentralized 'trust' architecture; but blockchain, in and of itself, cannot necessarily constitute a sound, robust, rigorous, trusted and authenticated 'chain of evidence' upon which to rely to prove apparently suspicious intent and possibly unlawful actions.

Illustrative References

[1] Examples:

https://link.springer.com/article/10.1007/s41109-019-0249-6

Quantitative analysis of cryptocurrencies transaction graph Amir Pasha Motamed & Behnam Bahrak Published: 30 December 2019

Introduction   Cryptocurrencies have made it possible for a financial system to perform transactions without the need for a centralized authority while keeping the transaction details and money generation clear and publicly available. Despite this transparency, people's identities are hidden, and they can transact anonymously. All transaction information of a cryptocurrency is usually stored in a distributed public ledger, named blockchain. The tasks of recording, updating, and maintaining the blockchain is the responsibility of network users for each coin, whose identities are unknown, and rewards have been created to provide them with sufficient incentives to do so, making the network up and running. Although the system is running by anonymous people, due to computational infeasibility of forging digital signatures and security of cryptography algorithms, transaction alteration is almost impossible. This level of security is guaranteed by cryptographic algorithms, and as long as these algorithms are secure, cryptocurrencies integrity is protected. …

https://www.researchgate.net/publication/277248535_Identifying_Bitcoin_users_by_transaction_behavior

Identifying Bitcoin users by transaction behavior Vinnie Monaco Naval Postgraduate School April 2015 DOI: 10.1117/12.2177039 Conference: SPIE DSS

ABSTRACT Digital currencies, such as Bitcoin, offer convenience and security to criminals operating in the black marketplace. Some Bitcoin marketplaces, such as Silk Road, even claim anonymity … This claim contradicts the findings in this work, where long term transactional behavior is used to identify and verify account holders. Transaction features, such as timestamp, coin-flow, and connectivity, contribute to revealing the account-holder's identity. The time between successive transactions is the result of low-frequency effects, such as the desire purchase an item and daily schedule, as well as higher frequency effects, such as hardware and network latency. In addition to transaction time-intervals, dynamic network features of each transaction, such as coin flow and number of edge outputs and inputs, can also be used to identify account-holders. In this paper, we propose novel methodology for identifying and verifying Bitcoin users based on the observation of Bitcoin transactions over time. … A subset of Blockchain 230686 is analyzed, selecting users that initiated between 100 and 1000 unique transactions per month for at least 6 different months. This dataset shows evidence of being nonrandom and nonlinear, thus a dynamical systems approach is taken. Identification and verification accuracies are obtained using monthly Bitcoin samples. Outgoing transactions, as well as both outgoing and incoming transactions, are considered. Results show an inherent lack of anonymity by exploiting patterns in long-term transactional behavior. …

https://www.frontiersin.org/research-topics/12966/cryptocurrency-transaction-analysis-from-a-network-perspective

Cryptocurrency Transaction Analysis from a Network Perspective

Cryptocurrencies …store their transactions publicly in blockchains. These longitudinal transaction records form large temporal networks of millions of nodes (addresses or accounts) and billions of edges (coin transfers or program function calls) connecting them together. They are probably the largest empirical datasets of complex networks, or graph data, publicly available. Cryptocurrencies have a wide adoption in (dark) markets and financial activities (for example, goods purchasing, fundraising, etc.), criminal activities (for example, fraud, money laundering, pyramid schemes, etc.) and gaming (for example, gambling, lottery, etc.). The public transaction records contain rich information and complete traces of these activities. …

https://www.chainalysis.com/professional-services/

Advanced blockchain forensics   Combining expertise in Chainalysis software, open source data analysis, and the latest investigative techniques, our team makes the cryptocurrency space safer by tackling the most challenging cases.

[2]
https://www.iso.org/committee/6266604.html
ISO/TC 307 Blockchain and distributed ledger technologies
Scope: Standardisation of blockchain technologies and distributed ledger technologies.
3 published ISO standards. 9 ISO standards under development under the direct responsibility of ISO/TC 307. 44 Participating members. 13 Observing members.

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

https://hackernoon.com/what-are-the-requirements-for-a-modern-crypto-wallet-fwt130jw
What Are the Requirements for a Modern Crypto Wallet? August 28th 2019 Kirill Shilov
Out of the 18 million of mined Bitcoins, nearly 27% are out of circulation, and most of those are supposedly lost. … the majority of them are lost due to mistakes in money management. That's why the importance of crypto wallets increases every day …   The first crypto wallet … was very simple: it allowed for the generation of new addresses and sending BTC to other people. No special measures were taken to protect or recover the private key, and it was easy to type an incorrect address and send coins to the wrong destination. …   The first exchange was launched in 2010, called Bitcoinmarket.com. The next year, 2011, was the year when Mt.Gox was launched, and people started to use it as some kind of a wallet. The Mt.Gox hack (when its users lost nearly 650,000 BTC) taught us not to store crypto on exchanges, and the demand for secure crypto wallets increased. Over time, many new wallets such as Exodus and Jaxx appeared, with multi-currency support and new security features. Nowadays, there are a lot of competing wallets for any currency …

https://www2.deloitte.com/mt/en/pages/technology/articles/mt-article-cryptocurrency-security-standard-CCSS.html
Cryptocurrency Security Standard (CCSS) By Sandro Psaila: IT Audit Senior Manager
As cryptos are expected to shift into the mainstream, one of the biggest challenges is confidence. Can CCSS bridge the gap? …   People and organisations are concerned about the authentication, authorisation and/or confidentiality limitations of cryptocurrency transactions. … By standardising the security techniques and methodologies used by crypto systems around the globe, end-users will be able to make educated decisions more easily about which products and services to use and with which companies they wish to align. On the other hand, many cryptos, like Bitcoin, are not governed by a central control point or "authority"; standardising on security will be a challenging process. … Although this standard has been around since 2014 and the number of crypto systems have mushroomed recently, very few organisations are claiming adherence with the CCSS when it comes to the management of crypto wallets. In fact, it is perceived that a considerable number of businesses in this space, mainly start-ups, do not follow security best practices, and their operations do not meet minimal security standards. …

[3]
'Blockchain vs Trust: The Fundamental Expert Dilemma', by Dr Stephen Castell, EXPERT WITNESS JOURNAL, WINTER 2019.

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 …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' … 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." …

Digital Bytes, Weekending 26th October 2019, TeamBlockchain Ltd.
http://www.teamblockchain.net/
… Binance's latest quarterly results … in the last two years it has made over $1billion of profit. CEO of Binance, Changpeng Zhao, … 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 … 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 …

'Code of practice and management guidelines for trusted third party services', S. Castell, INFOSEC Project Report S2101/02, 1993.
The APPEAL Report, Dr Stephen Castell, 1990, Eclipse Publications, ISBN 1-870771-03-6).

[4]
https://www.coinbase.com/legal/licenses#:~:text=Coinbase%2C%20Inc.%2C%20located%20at,State%20Department%20of%20Financial%20Services.
… Coinbase, Inc., located at 100 Pine St Suite 1250, San Francisco, CA 94111, is regulated and licensed as a money transmitter by the New York State Department of Financial Services. …
https://www.isregulated.com/coinbase-regulation-licensing-review/
"Coinbase is not under direct regulation by any authority or agency, … not considered unusual in the cryptocurrency market. ... North America's largest cryptocurrency exchange Coinbase is in talks with the Securities and Exchange Commission (SEC) to register as a licensed brokerage". 25 Feb 2020.
https://www.coindesk.com/uk-financial-service-provider-to-coinbase-bitstamp-awarded-fca-payments-license
UK Financial Service Provider to Coinbase, Bitstamp Awarded FCA Payments License
29 Jan 2020 - A company that provides financial services for cryptocurrency companies ... BCB Payments Ltd., is now the "first and only crypto-focused" company to have ... Institution license, meaning the firm is now regulated by the FCA.

https://sec.report/CIK/0001576711
Coinbase Inc.   SEC CIK #0001576711   Coinbase Inc. is registered with the U.S. Security and Exchange Commission and incorporated in the state of Delaware. For financial reporting, their fiscal year ends on December 31st. This page includes all SEC registration details as well as a list of all documents (S-1, Prospectus, Current Reports, 8-K, 10K, Annual Reports) filed by Coinbase Inc..

https://www.crunchbase.com/organization/poloniex
Poloniex is a cryptocurrency exchange with advanced trading features. Acquired by Circle.
https://www.crunchbase.com/organization/circle-2
Circle is a global internet finance company, built on blockchain technology and powered by crypto assets. Greater Boston Area, East Coast, New England.
https://poloniex.com/
The Legendary Crypto Asset Exchange
https://www.bloomberg.com/news/articles/2019-05-22/circle-cuts-10-of-staff-cites-restrictive-crypto-regulations
Circle Cuts 10% of Staff, Cites Restrictive Crypto Regulations By Julie Verhage 22 May 2019
https://www.bitdegree.org/crypto/poloniex-review
Poloniex Review: All-In-One Guide that Will Answer All of Your Questions
Poloniex is a cryptocurrency exchange that was first launched in 2014 by Tristan D'Agosta. The company's offices are located in Delaware in the U.S., meaning that they operate in a highly regulated nation. ... daily trading volumes of more than $100 million! 7 Sep 2020

https://www.sec.gov/Archives/edgar/data/1813793/000166357720000235/form10.htm

8.   Expert's Declaration and Statement of Truth

Expert's Declaration

I Stephen Peter Castell DECLARE THAT:

1. I understand that my duty in providing written reports and giving evidence is to help the Court, and that this duty overrides any obligation to the party by whom I am engaged or the person who has paid or is liable to pay me. I confirm that I have complied and will continue to comply with my duty.

2. I confirm that I have not entered into any arrangement where the amount or payment of my fees is in any way dependent on the outcome of the case.

3. I know of no conflict of interest of any kind, other than any which I have disclosed in my report.

4. I do not consider that any interest which I have disclosed affects my suitability as an expert witness on any issues on which I have given evidence.

5. I will advise the party by whom I am instructed if, between the date of my report and the trial, there is any change in circumstances which affects my answers to points 3 and 4 above.

6. I have shown the sources of all information I have used.

7. I have exercised reasonable care and skill in order to be accurate and complete in preparing this report.

8. I have endeavoured to include in my report those matters, of which I have knowledge or of which I have been made aware, that might adversely affect the validity of my opinion. I have clearly stated any qualifications to my opinion.

9. I have not, without forming an independent view, included or excluded anything which has been suggested to me by others, including my instructing lawyers.

10. I will notify those instructing me immediately and confirm in writing if, for any reason, my existing report requires any correction or qualification.

11. I understand that –

(a) my report will form the evidence to be given under oath or affirmation;

(b) questions may be put to me in writing for the purposes of clarifying my report and that my answers shall be treated as part of my report and covered by my statement of truth;

(c) the Court may at any stage direct a discussion to take place between experts for the purpose of identifying and discussing the expert issues in the proceedings, where possible reaching an agreed opinion on those issues and identifying what action, if any, may be taken to resolve any of the outstanding issues between the parties;

(d) the Court may direct that following a discussion between the experts that a statement should be prepared showing those issues which are agreed, and those issues which are not agreed, together with a summary of the reasons for disagreeing;

(e) I may be required to attend Court to be cross-examined on my report; and

(f) I am likely to be the subject of public adverse criticism by the judge if the Court concludes that I have not taken reasonable care in trying to meet the standards set out above.

Statement of Truth

I confirm that, insofar as the facts stated in this my **Expert's Report** are within my own knowledge, I have made clear which they are and I believe them to be true; and that the findings I have presented represent my true and complete professional analysis, conclusions and opinion for the purposes of such a report and all of the opinions expressed herein are opinions which I hold to a reasonable degree of scientific certainty.

Signature

....

Date

....

Dr Stephen Castell, *CASTELL Consulting*   **19 October 2020**